UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

EVALUACIÓN DE HERRAMIENTAS TIC PARA GESTIONAR EL MONITOREO Y ANÁLISIS DE LA RED DE DATOS DEL RECINTO DE GOLFITO DE LA UNIVERSIDAD DE COSTA RICA

Trabajo final de investigación aplicada sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Maestría Profesional en Tecnologías de Información y Comunicación en la Gestión Organizacional para optar al grado y título de Maestría Profesional en Tecnologías de Información y Comunicación en la Gestión Organizacional

ALAN MARTÍN CORRALES RODRÍGUEZ

Ciudad Universitaria Rodrigo Facio, Costa Rica. 2020

Dedicatoria

Este trabajo es dedicado a mi familia y pareja por el apoyo antes y durante el proceso de realización.

Agradecimiento

Agradecimiento para todos las personas que de alguna o otro forma inspiraron y colaboraron para la creación de este trabajo, especialmente a mi familia y pareja.

“Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudio de Posgrado en tecnologías de información y comunicación para la gestión organizacional de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en tecnologías de información y comunicación para la gestión organizacional.”

FRANCISCO JOSE BLANCO CHAVARRIA (FIRMA)
Firmado digitalmente por FRANCISCO JOSE BLANCO CHAVARRIA (FIRMA)
Fecha: 2020.05.13 14:14:39 -06'00'

M.Sc. Francisco Blanco Chavarría

Representante del Decano Sistema de Estudio de Posgrado

SINDY PORRAS SANTAMARIA (FIRMA)
Firmado digitalmente por SINDY PORRAS SANTAMARIA (FIRMA)
Fecha: 2020.05.13 19:43:00 -06'00'

M.Sc. Sindy Porras Santamaría

Profesora Guía

OSCAR MARIO ALFARO SOLIS (FIRMA)
Digitally signed by OSCAR MARIO ALFARO SOLIS (FIRMA)
Date: 2020.05.13 21:38:42 -06'00'

M.B.A. Oscar Alfaro Solís

Lector

RAFAEL ANTONIO MARTINEZ VILLARREAL (FIRMA)
Firmado digitalmente por RAFAEL ANTONIO MARTINEZ VILLARREAL (FIRMA)
Fecha: 2020.05.13 18:08:01 -06'00'

M.Sc. Rafael Martinez Villareal.

Lector

YORLENY SALAS ARAYA (FIRMA)
Firmado digitalmente por YORLENY SALAS ARAYA (FIRMA)
Fecha: 2020.05.13 22:29:04 -06'00'

M.Sc. Yorleny Salas Araya

Directora del Programa de Posgrado

ALAN MARTIN CORRALES RODRIGUEZ (FIRMA)
Firmado digitalmente por ALAN MARTIN CORRALES RODRIGUEZ (FIRMA)
Fecha: 2020.05.13 13:51:21 -06'00'

Alan Martín Corrales Rodríguez

Sustentante

Indice

Resumen

Se propone a evaluar opciones de herramientas TIC como solución a los requerimientos de monitoreo y seguridad. Con el desarrollo de este trabajo de investigación se pretende brindar una guía al Recinto de Golfito de opciones de herramientas TIC elaboradas para dar solución a los requerimientos de monitoreo y seguridad que sera previamente evaluadas, y que podráa ser de utilidad también para otras sedes y recintos de la UCR.

Lo que se pretende lograr registrar con el monitoreo y análisis de red de datos la medición del rendimiento, carga y seguridad, logrando una comprensión de la información por medio de la facilidad de lectura, dar solución a potenciales problemas de seguridad y privacidad, y mejora de la relación organización-usuario, al conocer sus necesidades y factores influyentes en el comportamiento dentro de la red. Por ende, la toma de decisiones puede ser mas acertada para los administradores RID y directivos de la organización, con el uso de la muestra de datos verídicos e información estratégica.

Índice de figuras

Índice de tablas

UNIVERSIDAD DE COSTA RICA

SEP Sistema de Estudios de Posgrado

Autorización para digitalización y comunicación pública de Trabajos Finales de Graduación del Sistema de Estudios de Posgrado en el Repositorio Institucional de la Universidad de Costa Rica.

Yo, Alan Corrales Rodríguez, con cédula de identidad 603680225, en mi condición de autor del TFG titulado Evaluación de herramientas TIC para gestionar el monitoreo y análisis de la red de datos del Recinto de Golfito de la UCR

Autorizo a la Universidad de Costa Rica para digitalizar y hacer divulgación pública de forma gratuita de dicho TFG a través del Repositorio Institucional u otro medio electrónico, para ser puesto a disposición del público según lo que establezca el Sistema de Estudios de Posgrado. **SI** [X] **NO** *[ ]

***En caso de la negativa favor indicar el tiempo de restricción: _____ año (s).**

Este Trabajo Final de Graduación será publicado en formato PDF, o en el formato que en el momento se establezca, de tal forma que el acceso al mismo sea libre, con el fin de permitir la consulta e impresión, pero no su modificación.

Manifiesto que mi Trabajo Final de Graduación fue debidamente subido al sistema digital Kerwá y su contenido corresponde al documento original que sirvió para la obtención de mi título, y que su información no infringe ni violenta ningún derecho a terceros. El TFG además cuenta con el visto bueno de mi Director (a) de Tesis o Tutor (a) y cumplió con lo establecido en la revisión del Formato por parte del Sistema de Estudios de Posgrado.

INFORMACIÓN DEL ESTUDIANTE:

Nombre Completo: Alan Corrales Rodríguez.

Número de Carné: A61773 Número de cédula: 603680225.

Correo Electrónico: alan.corralesrodriguez@ucr.ac.cr.

Fecha: 10/5/2020. Número de teléfono: 87129209.

Nombre del Director (a) de Tesis o Tutor (a): Sindy Porras Santamaría.

FIRMA ESTUDIANTE

Nota: El presente documento constituye una declaración jurada, cuyos alcances aseguran a la Universidad, que su contenido sea tomado como cierto. Su importancia radica en que permite abreviar procedimientos administrativos, y al mismo tiempo genera una responsabilidad legal para que quien declare contrario a la verdad de lo que manifiesta, puede como consecuencia, enfrentar un proceso penal por delito de perjurio, tipificado en el artículo 318 de nuestro Código Penal. Lo anterior implica que el estudiante se vea forzado a realizar su mayor esfuerzo para que no sólo incluya información veraz en la Licencia de Publicación, sino que también realice diligentemente la gestión de subir el documento correcto en la plataforma digital Kerwá.

Introducción

Objetivo general

Recomendar herramientas TIC para el monitoreo y análisis de los datos de la red con el fin de mejorar la gestión de la red de datos del Recinto de Golfito.

Objetivos específicos

- Identificar herramientas TIC para el monitoreo y análisis de datos de la red con el fin de conocer las opciones disponibles para su posterior análisis.
- Analizar documentación y funcionamiento de las herramientas TIC para el monitoreo y análisis de datos de la red con el fin de elegir cuáles comparar.
- Comparar las herramientas TIC para el monitoreo de los datos en la red con el propósito de identificar las fortalezas y debilidades de cada una.
- Evaluar herramientas TIC para el monitoreo y análisis de datos con el fin de mejorar la gestión de la red de datos del Recinto de Golfito.

Justificación

Como parte del desarrollo económico, social y cultural, la sociedad se ve impulsada a la utilización de medios de comunicación viables y rentables en sus actividades, con la adquisición de productos y servicios de calidad que brinden una vida digna acorde a las necesidades y gustos de la población. Por ende, son indispensables aspectos como la seguridad, privacidad y calidad del producto en el uso cotidiano de la tecnología. Como mencionan Amoroso y Costales (2016):

> En los momentos actuales no se puede ver al hombre alejado de la tecnología, donde el primero aparece ante el recurso información no solo como un agente pasivo, que se nutre del entorno y de aquello que este le

> ofrece; sino que también funciona como agente activo: productor de información. (p. 4).

Actualmente, en nuestro país casi toda persona está conectada por medio de algún dispositivo electrónico a la red de datos, sea pública o privada, teniendo acceso a una producción masiva de paquetes digitales (conjunto de datos que consta de información a comunicar y datos para su control y comunicación). Según el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) en la *Encuesta de acceso y uso de los servicios de telecomunicaciones en Costa Rica 2017*, el “90% de las personas indican que utilizan Internet todos los días o casi todos los días” (p. 36). La información generada se hace cada vez más pertinente en el proceso de toma de decisiones de las empresas e instituciones gubernamentales.

Las tecnologías de la información y comunicación (TIC) se pueden apreciar, por ejemplo, en la administración de recursos humanos, económicos, de investigación, control de inventarios y análisis de mercados, por mencionar áreas de importancia en las empresas.

Debido a esta relación y la creación de nuevas formas de comunicar dentro del contexto que se desarrolla, se muestra la necesidad de proyectar a las empresas e instituciones medidas de promoción de seguridad y privacidad de la información para sus colaboradores, empezando por el comportamiento de los usuarios en la red de datos. A partir de esto, se generan en el proponente las siguientes interrogantes:

- ¿Mediante cuáles dispositivos estamos teniendo acceso a la información?
- ¿Cuáles son los tiempos de uso de la red de datos?
- ¿Cuál es el consumo de contenido acorde a las labores o bien recreaciones?
- ¿Qué tan fiables son los medios de comunicación digitales?

- ¿Qué importancia tiene para el usuario resguardar su información personal y corporativa?

Conocer la respuesta a dichas preguntas es lo que persigue esta investigación, con miras a generar un marco de referencia que nos respalde para la toma de decisiones.

En cuanto al manejo de datos, Amoroso y Costales (2016) expresan que:

> El aumento desmesurado de datos y la información pública han contribuido al surgimiento de nuevos paradigmas o herramientas; como el Big Data, el cual no se puede divorciar de la apertura de los datos (Open Data), a pesar de ser temas muy novedosos los resultados obtenidos de su aplicación en diferentes sectores han hecho de ambos paradigmas un elemento clave en el desarrollo de la sociedad de la información en su tránsito a la sociedad del conocimiento. (p.4)

La existencia de estas herramientas está en manos de las empresas como soluciones a corto y mediano plazo en análisis, monitoreo, control y aseguramiento de la red. Sin embargo, se ha dado la apertura de nuevos retos, tales como solventar una mayor escalabilidad y sostenibilidad de las TIC como un medio afianzado para alivianar los procesos de toma de decisiones. Por su parte, la implementación de herramientas para la estadística de redes es muy reciente, debido a esto se pueden encontrar problemas durante el desarrollo; sin embargo, ha aumentado su soporte y guía con los años, brindando mayor confiabilidad en su uso.

La estadística en la computación conlleva la manipulación de la información dentro las corporaciones, provocando el uso masivo de algoritmos para la toma de decisiones en el día a día de las corporaciones modernas, por lo cual se hace cada vez más importante no solo contar con técnicos, sino también profesionales capacitados en la interacción humana y creación de contenido en pro de la automatización de procesos dentro de las empresas: “Los fines son lícitos, pero

debe tenerse presente que el tratamiento de la información tiene implicaciones éticas cuando se trata de datos sobre personas.” (Franganillo, 2009). Esto nos remite a la importancia de crear políticas en cuanto al uso y control de la información, ya que no puede quedar en manos de cualquier persona y competencia.

En la mayoría de las empresas es importante administrar la privacidad y la seguridad no solo de la información y de los usuarios. Esta necesidad legal en Costa Rica se encuentra resguardada por la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, ley número 8968, la cual menciona en su primer artículo lo siguiente:

> ARTÍCULO 1.- Objetivo y fin Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Como bien se denota, acorde a la actualización de los medios digitales, es importante actualizar las leyes y políticas públicas y privadas en el tratamiento de los datos, y en Costa Rica no es para menos.

Como menciona The Software Alliance, (2015) en su informe titulado Estudio de los Datos:

> Un desafío que debería ser una de las principales prioridades tanto para la industria como para el gobierno es calmar la preocupación de que se usen los datos de manera injusta respecto de algunas personas o clases de personas. Al mismo tiempo, hay oportunidades que no deben pasarse por alto a la hora de usar los datos para combatir la discriminación injusta y darles poder a los grupos. De

> hecho, si se usan de manera responsable, los datos pueden ser una poderosa herramienta nueva para dejar al descubierto los actos de discriminación actuales que afectan el acceso a los empleos, las finanzas, la educación y las oportunidades. (p. 2)

Es importante destacar que la manipulación de los datos y la información procesada es de valor si se comparte con otros para la toma de decisiones y mejoras constantes, siempre que esto no ponga en peligro la seguridad de la organización. En el informe de The Software Alliance (2015) indica que:

> Las normas gubernamentales actuales en materia de privacidad se pueden combinar con avances rigurosos e innovadores en la privacidad y buenas prácticas voluntarias de la industria para garantizar que los datos estén seguros y que se proteja la información personal. Por el contrario, las órdenes gubernamentales que intentan abordar la privacidad y la seguridad mediante la exigencia de que los datos se almacenen localmente podrían inhibir la innovación y limitar los tipos de beneficios sociales que la innovación de los datos puede producir. (p.4)

Según Amoroso y Costales (2016):

> La principal fuente de retroalimentación para sentar las bases para aplicación del análisis de los grandes datos generados por el entorno está en establecer una fuerte colaboración entre los organismos de Administración Pública, y los ciudadanos, con el principal objetivo de ayudar a definir una guía política siempre orientada a lograr la eficiencia y la agilidad de los procesos burocráticos; es fundamental ubicar el factor tecnológico como punto medio entre ambas partes con la finalidad de agilizar la gestión de la documentación, la información y los datos generados por cualquiera de las partes, así como viabilizar los flujos de información, el acceso y el intercambio continuo. (p. 4).

Como menciona el en la cita, la institución pública no está exenta del uso de las TIC como medio para agilizar los procesos gubernamentales y esto se logra con la aplicación diaria de análisis y toma de decisiones.

En el Recinto de Golfito de la Universidad de Costa Rica (UCR) se presenta la necesidad de contar con TIC que brinden más información para la toma de decisiones en la Oficina de Informática, pues gran parte de estas se basan en el uso y rendimiento de la red de datos local; por consiguiente, se buscan herramientas para poder hacer el monitoreo y análisis de la red de datos, y es aquí donde la implementación de software de predicción y analítica puede brindar una solución.

En toda empresa se ve la necesidad de regular cuanto haga referencia a la informática. Para los administradores de Recursos Informáticos Desconcentrados (RID) de la UCR, está la necesidad de crear pasos a cumplir, protocolos de información, configurando los sistemas y equipos con políticas y dominios propios, para el filtrado de la información o priorización de esta. De modo que resulta oportuno crear políticas corporativas por el comportamiento y uso de la red de datos de usuarios, tomando en cuenta el manejo de los sistemas de información, y controlando así la imagen y fuga de información.

Según García y Valcárcel (2015) indican que:

> “Existe una gran variedad de herramientas que permiten realizar los procesos de captura de tráfico y el procesamiento. Sin embargo, ninguna es mejor que el resto de forma absoluta, si no que cada una es ventajosa en diferentes situaciones.” (p.6)

Debido a las ventajas que nos dan las TIC, se hace necesario el uso de recursos en línea y almacenamiento local en el campo de investigación. Durante el proyecto, este proponente pretende probar varias herramientas TIC simultáneamente, para el monitoreo y análisis de la red de datos local del Recinto de Golfito, con el propósito de gestionar un ahorro de recursos económicos debido al uso de plataformas y herramientas de código libre y de licenciamiento libre.

Para ello se propone evaluar opciones de herramientas TIC como solución a los requerimientos de monitoreo y seguridad. Con el desarrollo de este trabajo de investigación, se pretende brindar una guía al Recinto de Golfito con opciones de herramientas TIC elaboradas para dar solución a los requerimientos de monitoreo y seguridad que serán previamente evaluadas. Asimismo, dicha guía podría ser de utilidad también para otras sedes y recintos de la UCR.

Lo que se pretende es 1- lograr registrar con el monitoreo y análisis de red de datos la medición del rendimiento, carga y seguridad, logrando una comprensión de la información por medio de una fácil lectura, 2- dar solución a potenciales problemas de seguridad y privacidad, y 3- mejorar la relación organización-usuario, al conocer sus necesidades y factores influyentes en el comportamiento dentro de la red. Por ende, la toma de decisiones puede ser más acertada para los administradores RID y directivos de la organización, con el uso de la muestra de datos reales e información estratégica.

Es importante tener cuidado al manipular datos de nuestra organización, ya que detrás de todos esos datos existen personas; por ende, se debe procurar un manejo correcto de la información, con transparencia en los procesos de acceso, almacenamiento, exploración y análisis de los datos recaudados por medio de software y cuestionarios. La recolección de la información se busca con el consentimiento de la unidad auditada, siendo esta los usuarios y la jefatura administrativa, cuyos datos serán los utilizados en la investigación.

En la captura de paquetes de datos por medio de herramientas como Wireshark, Ntop, Tcpdump, y monitoreo de red con Nagios y Scrutinizer, se puede comprender una interpretación del uso y consumo de datos de la red; sin embargo, cuando la cantidad capturada es masiva y se hace por tiempos prolongados es necesario almacenar e interpretar usando herramientas más complejas como minería de datos, brindando la posibilidad de realizar estudios estadísticos a los datos y convertirlos en información válida y legible.

Marco teórico

El desarrollo de este TFIA se enfoca en la búsqueda de herramientas TIC para el monitoreo y análisis de datos, que colaboren en el uso y comportamiento del usuario en la red de datos local del Recinto de Golfito, punto de partida para entender a grandes rasgos el concepto de términos y tecnologías a utilizar.

Tecnologías de información y comunicación en la seguridad organizacional

Las nuevas tecnologías de la información y comunicación (TIC) giran en torno a la informática, la microelectrónica y las telecomunicaciones de forma interactuada, lo que permite además de un medio de comunicación, el desarrollo personal, organizacional y social.

La comunicación orienta a los colaboradores de una organización a trabajar por objetivos en común, mediante acuerdos, relaciones y políticas consensuadas; es ahí donde las TIC juegan un papel primordial en la gestión y control de la información, por medio de la adquisición e implementación de equipo especializado y de sistemas para la organización y transmisión de datos.

En las organizaciones, las TIC se presentan como un medio para resolver tareas y labores a los usuarios como consumidores y productores de contenido, quienes pueden estar expuestos a grietas en la seguridad, exponiendo los datos de las organizaciones ante la competencia y criminales cibernéticos.

Según el informe de seguridad informática ESET Security Report 2018, se detalla un aumento constante de problemas de seguridad y privacidad en las organizaciones latinoamericanas. Las cuatro categorías de mayor influencia en la seguridad informática son: en primer lugar, está el secuestro de datos (57%), de segundo se encuentra la explotación de vulnerabilidades (55%), de tercero los programas maliciosos (53%) y de cuarto el robo de información (51%). Como se evidencia, la tecnología no solo se trata de usarla y crear contenido sin control alguno, al tratar la información con el valor que se requiere se puede mejorar su

protección, además de la forma en cómo se usa y su análisis para la toma de decisiones organizacionales.

En las organizaciones ya se habla de implementar controles de seguridad, posiblemente sean muchas las soluciones, desde incluir políticas y planes de contingencia para gestión de la información, hasta medidas de seguridad a nivel de hardware y software. Hay claridad acerca de la importancia de tomar medidas para proteger una fuente principal de información, pero es primordial educar al usuario en los diferentes niveles jerárquicos.

Como plantean Slusarczyk *et al.* (2013):

> Actualmente las TIC son la fuente principal de información para la empresa y la información es un recurso estratégico muy importante que sustenta las funciones claves y los procesos de toma de decisiones. Para la toma de decisiones de calidad es indispensable que el negocio cuente con los datos necesarios, como también con adecuado tratamiento y análisis de estos datos. La manera como la información se gestiona, incluyendo la tecnología utilizada para apoyarlo, es, por tanto, fundamental para las prácticas comerciales. (p. 39).

La implementación de herramientas TIC en el Recinto de Golfito es parte de un esfuerzo de gestión y control de los administradores RID en conjunto con el área administrativa. Su funcionamiento conlleva esfuerzo, tiempo y análisis, por eso es importante la interacción que la información pueda brindar en la toma de decisiones.

Captura y monitoreo de la red de datos local.

Las organizaciones dependen directamente de la disponibilidad de la red de datos, con un correcto monitoreo y captura de datos se pueden tomar decisiones sobre los usos de la red. Según la empresa PandoraFMS (Martín, 2017), las razones principales por las que se deberían monitorear todos los sistemas informáticos son las siguientes:

- Acceder al estado de los sistemas informáticos en tiempo real.
- Detectar el origen de los incidentes.
- Acceder a información ejecutiva del estado de las instalaciones y chequear cómo están los activos informáticos más críticos.
- Mejorar la eficacia y la eficiencia de las labores de mantenimiento del sistema.
- Configurar eventos y alarmas. Por ejemplo, alarmas cuando un disco duro esté lleno, la memoria esté ocupada por encima del 80%, en caso de que haya demasiados accesos a disco en modo escritura, demasiados hilos abiertos corriendo en el mismo sistema, etc.
- Inventariar sistemas (mapas, listados).
- Planificar el crecimiento con base en el uso real de los sistemas. Mediante informes de uso, se pueden detectar tendencias y saber cuándo hace falta más disco, poner otro servidor o aumentar la memoria.
- Reducir costes.

Con la apertura de nuevas tecnologías de código abierto y licenciamiento libre se tiene acceso a herramientas para los distintos trabajos de informática. En el caso de captura y monitoreo de datos en la red de datos local, se tiene acceso a software especializado y de altas prestaciones para dicha labores. Las herramientas a considerar son usadas en ambientes de trabajo con altas demandas en rendimiento y estabilidad, y en el caso de implementarlas en el Recinto de Golfito no va a ser la excepción. Al usar herramientas TIC libres, estas no solo brindan acceso casi inmediato sin problemas de licenciamiento o relativamente gratis; además, permiten un conjunto de soluciones apegadas a la necesidad de control y gestión de la información en la unidad auditada.

Captura y monitoreo

Para la captura y monitoreo de los datos que se pretende realizar, es importante conocer las técnicas más acordes a los requerimientos, por consiguiente, se explican de forma puntual las técnicas de monitoreo que se podrían implementar.

Monitoreo activo

Este tipo de monitoreo se realiza introduciendo paquetes de pruebas en la red o enviando paquetes a determinadas aplicaciones y midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red y es empleado para medir su rendimiento. A continuación, se explican algunos de los protocolos en los que se basa este monitoreo y lo que ofrece cada uno.

Basado en ICMP (Internet Control Message Protocol):

- Diagnosticar problemas en la red.
- Detectar retardo, pérdida de paquetes.
- RTT (Round-Trip delay Time).
- Disponibilidad de host y redes.

Basado en TCP (Transmission Control Protocol):

- Tasa de transferencia.
- Diagnosticar problemas a nivel de aplicación.

Basado en UDP (User Datagram Protocol):

- Pérdida de paquetes en un sentido (one – way).
- RTT (tracerroute).

Monitoreo pasivo

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como programas informáticos que registran la información que envían los periféricos (sniffers),

ruteadores, computadoras con software de análisis de tráfico y en general, dispositivos con soporte para SNMP (Simple Network Management Protocol), RMON (Remote Network MONitoring) y herramientas de monitorización de banda ancha, como el Netflow. Este enfoque no agrega tráfico a la red como lo hace el activo y es utilizado para caracterizar el tráfico en la red y para contabilizar su uso.

Captura de tráfico

Por medio de la configuración de un puerto espejo en un dispositivo de red, se hace una copia del tráfico recibido en un puerto hacia otro donde estará conectado el equipo que realizará la captura.

Se requiere la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red.

Técnicas del análisis del tráfico

En el proceso de este trabajo de investigación, se pretende el análisis de datos capturados en la red local del Recinto de Golfito. Parte de la labor consiste en explorar la información en busca de parámetros que nos permitan clasificar y seleccionar la información de valor en la toma de decisiones.

Para realizar dichas labores se usarán técnicas y métodos de análisis de información, los cuales se describen a continuación.

Visualización de datos

Como lo describen en Tableau Software (2019):

> La visualización de datos es una representación gráfica de la información y los datos. Mediante el uso de elementos visuales, como gráficos y mapas, la visualización de datos ofrece una manera accesible para detectar y comprender las tendencias, los valores atípicos y los patrones en los datos.

> En el mundo de los big data, las herramientas y las tecnologías de visualización de datos son esenciales para analizar cantidades masivas de información y tomar decisiones basadas en los datos. (p.2)

Para efectos de este TFIA, la visualización de datos es primordial, ya que brinda una exposición más legible de los análisis y sus respuestas, para la toma de decisiones en el desarrollo de medidas de seguridad en la red de datos, creación y actualización de políticas, además en compra de equipo de cómputo y comunicación para el Recinto de Golfito.

Análisis de escenarios

Con el análisis de escenarios se busca ampliar la perspectiva de los posibles entornos que se encuentren durante la exploración de información, contemplar las futuras consecuencias y prevenir o limitar las acciones. Se trata de responder todas las preguntas que se puedan generar durante el proceso de estudio de la red de datos del Recinto.

Para Jordán (2016):

> La utilidad del análisis de escenarios es su apoyo a la planificación estratégica: contribuye a identificar señales de alerta temprana, a valorar la fortaleza de las competencias nucleares de la propia organización, a generar opciones estratégicas mejores y a evaluar el riesgo de cada opción estratégica a partir de las incertidumbres identificadas. (p. 3).

Análisis de sentimiento

Al querer descubrir posibles brechas de inseguridad en la red de datos y en el comportamiento del usuario al usar los recursos tecnológicos de la UCR, es importante clasificar esta información que al no ser estructurada lleva un proceso diferente, pero no alejado del estudio y de las herramientas tecnológicas.

Gamboa (1999), en su presentación de análisis de sentimientos para la toma de decisiones, menciona que el análisis de sentimiento:

> Es el análisis de información no estructurada, la cual se puede encontrar en redes sociales. Usa técnicas de Lingüística, modelamientos estadísticos y técnicas de aprendizaje para descubrir conocimientos que no existen explícitamente en ningún texto de la colección, pero que surgen al relacionar el contenido de muchos de ellos. Se busca entender al usuario, descubrir las bases de su conocimiento y como se aplica ese conocimiento en las labores diarias. (p. 5).

Herramientas para la captura y análisis de la red de datos local

La instalación y configuración de herramientas para la captura y análisis de información en la red de datos local, se puede dividir en cuatro grupos de software:

- Sniffer: hace una captura en tiempo real de los datos en transmisión.
- Sistemas de monitoreo: ayudan a controlar y gestionar los equipos y conexiones existentes en la red de datos
- Analizadores de captura: implementan, como su nombre lo dice, el análisis de las capturas del tráfico de red realizadas por un Sniffer
- Minería de datos: proporcionan información más detallada que pasamos por alto en los análisis de la red de datos y que sin dudas nos pueden brindar detalles importantes para la toma de decisiones.

Sniffer

Como menciona el blog Mundo Cisco (2009), un sniffer es un programa de captura de las tramas de red. Es algo común que el medio de transmisión (cable coaxial, UTP, fibra óptica, entre otros) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguirlo el Sniffer le dice a la computadora que deje de ignorar todo el tráfico no destinado al equipo y le ponga

atención, lo cual es conocido como poner en estado "*promiscuo*" a la NIC (Network Interface Card).

En la actualidad la seguridad en las redes es de vital importancia, ya que toda la información que se transmite a través de estas muchas veces puede ser utilizada para fines de lucro o realizar delitos electrónicos.

Algunas aplicaciones sniffer son: Wireshark, Netsniff-ng, Tcpick, Justniffer, CapTipper, Tcpdump.

Analizadores de captura de datos

Se trata de herramientas de análisis forense de red en su mayoría multiplataforma. También permiten observar los archivos Pcap para el análisis fuera de línea y regenerar o reensamblar los archivos transmitidos y los certificados de los archivos Pcap. Además, filtran la información que van encontrando y la exponen de una forma clara y rápida gracias a su interfaz gráfica.

Algunas aplicaciones de análisis son: Network Miner, Xplico, Bro-IDS, Dripcap, Capanalysis, PcapXray, TNV, Deplug, NetworkTotal, PcapXray.

Sistemas de monitoreo

Se refiere a sistemas integrados que permiten la gestión de redes de manera más rápida e inteligente. De forma predefinida, ofrecen monitorización de redes de servidores físicos y virtuales, análisis de ancho de banda basado en flujo, análisis y almacenamiento de logs de firewall, gestión de cambios y configuraciones, y administración de direcciones IP y puertos de switch, brindando de esta manera toda la visibilidad y control que necesita sobre su red.

Algunas aplicaciones de monitoreo son: Nagios, Manege Engine, ntop, Snort, Suricata, OSSEC, Sguil, Squert, CapMe, ELSA.

Minería de datos

La minería de datos es también denominada extracción de datos. Se refiere a la práctica por medios automáticos o semiautomáticos de la búsqueda y la exploración en grandes almacenes de datos de relaciones no visualizadas previamente, dando por resultado el descubrimiento de patrones significativos entre los mismos y reglas. Para lograr este propósito, la minería de datos emplea técnicas estadísticas de automatización del conocimiento y de reconocimiento de patrones (observar datos de una sola fuente, recursos de información, etc.) (De la puente, 2010).

Algunas aplicaciones de minería de datos son: Rapid Miner, Orange, Maltengo CE.

Leyes y políticas sobre la privacidad de datos

El uso de las TIC se ha visto presente en todas las áreas de la sociedad y en cada espacio de interacción. Hoy en día es casi imposible concebir algún proceso sin pensar en el uso de la informática (Chen, 2007). Esto no excluye que tanta producción de contenido e intercambio de información llame la atención de quienes buscan la forma de realizar estafas, robo de información, aprovechamiento de controles y acceso a ella ilícitamente.

Es importante la existencia de legislación tanto nacional como internacional, que en conjunto ayude a la protección de la persona ante delitos informáticos y control de la privacidad. En el informe de cyberseguridad de ESET, Seger (2016) afirma que:

> La efectividad de la justicia penal es parte esencial de una estrategia de seguridad cibernética. Esto comprende la investigación, la fiscalización y la adjudicación de delitos en contra y por medio de datos y sistemas informáticos, al igual que la obtención de evidencia electrónica relacionada con cualquier delito, para propósitos del proceso penal. La naturaleza transnacional del delito cibernético y en particular la volatilidad de la evidencia electrónica implica que la justicia penal no puede ser efectiva sin una cooperación internacional eficiente. (p. 19).

Una formulación correcta de leyes y políticas en la justicia penal del delito cibernético debe estar actualizada y ser pertinente con las nuevas técnicas y medios utilizados por los criminales cibernéticos, no solo en el robo de datos y programas maliciosos; además, debe estar en beneficio de la integridad personal de los usuarios de la red de redes.

Es importante que el uso de las TIC esté de la mano de los derechos humanos de los usuarios, en el entendido de que los derechos humanos son el instrumento normativo que permite garantizar y llevar a cabo evaluaciones de los progresos en la seguridad de las personas a través de diferentes acciones estatales, como lo son la formulación e implementación de políticas o estrategias nacionales de seguridad digital (Sequera, 2018).

Leyes internacionales

En el ámbito internacional existe una diversidad de leyes y normativas para la regulación sobre la privacidad y seguridad la información; en el caso del desarrollo de este TFIA solo se citan algunas leyes:

- Convenio de Budapest: el Convenio de Budapest es un instrumento internacional que busca homogeneizar la manera en que los diversos países contratantes abordan y definen la cibercriminalidad. Según el Observatorio de Seguridad en América Latina y el Caribe (2016), “el Convenio de Budapest, por lo tanto, puede servir de lista de verificación para el desarrollo de leyes internas sustantivas y procesales relativas al delito cibernético y la electrónica. Tal parece que más de 130 Estados en el mundo lo han usado como directriz de una forma u otra. Sin embargo, el Convenio en su totalidad es un documento balanceado, juicioso y coherente y debe considerarse preferiblemente como un todo” (p. 21).

- La normativa ISO 27032 es un nuevo estándar de ciberseguridad publicado en julio de 2012 por la Organización Internacional de Normalización (ISO).

- La Norma ISO/IEC 27032:2012 "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad" ofrece unas líneas

generales de orientación para fortalecer el estado de la Ciberseguridad en una empresa, utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados con:

- La seguridad en la redes.
- Seguridad en Internet.
- Seguridad de la información.
- Y la seguridad de las aplicaciones.

Leyes gubernamentales de Costa Rica

El año 2012 fue un año decisivo para la seguridad cibernética en Costa Rica con la aprobación de la Ley 9048, la cual introdujo formalmente el delito cibernético al Código Penal del país. Costa Rica también reconoce la Convención Interamericana sobre Asistencia Mutua en Materia Penal (comúnmente conocida como la “Convención de Nassau”) y regularmente coordina con la Interpol. Los ciudadanos en general gozan de la protección de la libertad de expresión y los derechos a la privacidad bajo la jurisdicción interna (Observatorio de Seguridad en América Latina y el Caribe, 2016).

Con la Ley 9048 de Delitos Informáticos se establecen reformas y modificaciones al Código Penal, entre ellas, nuevos tipos penales como suplantación de identidad, suplantación de páginas electrónicas e instalación o propagación de programas informáticos maliciosos. También se contemplan otros delitos como la violación de correspondencia y datos personales, extorsión, estafa informática, daño informático y espionaje. Con lo anterior, se busca no solo la protección de personas físicas, sino también de personas jurídicas (Velásquez, 2012).

El Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) de Costa Rica es la autoridad principal responsable del manejo de los problemas y del desarrollo de políticas relacionadas con la seguridad cibernética nacional. Otras instituciones, incluida la Secretaría Digital/Gobierno Digital, la sección de Delitos Informáticos del Poder Judicial, la Superintendencia de Telecomunicaciones, el Banco Central y

la Agencia de Protección de Datos de los Habitantes (Prodhab), también han sido clave en esta área. El MICITT está en las etapas iniciales de la planificación de una estrategia de seguridad cibernética nacional (Observatorio de Seguridad en América Latina y el Caribe, 2016).

Directrices institucionales

A partir de 2015, en la UCR se reconoce la importancia de adoptar un conjunto de directrices técnicas de seguridad de información, enfocadas en la protección de la información perteneciente a la Universidad o en su custodia, con el objetivo de lograr un manejo eficiente de los recursos, mejoramiento constante de los servicios y labores de la institución. manejo eficiente de los recursos, mejoramiento constante de los servicios y labores de la institución.

Las Directrices Técnicas de Seguridad de Información de la UCR se fundamentan en la documentación de Directrices Técnicas para Gestión y el Control de la Tecnologías de la Información (N-2-2007 CO-DFOE).

La Universidad de Costa Rica

La Universidad de Costa Rica es una institución de educación superior abanderada de la enseñanza humanista. El 12 de marzo de 2001 los diputados y diputadas de la Asamblea Legislativa, tomando en cuenta el aporte de la institución de educación al país, la declaran Institución Benemérita de la Educación y la Cultura Costarricense mediante la Ley Nº 8098. Desde su constitución en 1940, esta institución goza de autonomía universitaria.

En el artículo 1 del Estatuto orgánico de la Universidad de Costa Rica se puntualiza que:

> La Universidad de Costa Rica es una institución de educación superior y cultura, autónoma constitucionalmente y democrática, constituida por una comunidad de profesores y profesoras, estudiantes, funcionarias y funcionarios administrativos, dedicada a la enseñanza, la investigación, la

> acción social, el estudio, la meditación, la creación artística y la difusión del conocimiento. (1974, p. 1).

Recinto de Golfito

Con la adquisición de las antiguas instalaciones de la Compañía Bananera de Costa Rica (CBCR), la Universidad obtuvo un activo importante para generar un mayor posicionamiento en la región, ya que posibilita la gestión de distintos procesos de logística en proyectos de investigación, acción social y docencia. Como se menciona en la propuesta académica del del Recinto de Golfito en el 2010, elaborada por un grupo de docentes y administrativos apoyado en datos de la oficina de Informática, para 1988 se produce un cambio de proyección, ya que en la sesión 3512 del Consejo Universitario se autorizó al rector de turno para que "traspasara en usufructo las instalaciones de Golfito a la Fundación para la Cooperación Interuniversitaria en el Pacifico (FUCIP)". Este traspaso tuvo validez hasta el año 1999, cuando las instalaciones pasaron a ser administradas por la Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI). En el año 2004, la nueva junta administradora consideró que estas instalaciones, por ser bienes públicos, deben ser administradas por las diferentes instancias de la Universidad de Costa Rica.

Para el año 2005, se logró consolidar la idea del Recinto como proyecto académico, iniciando con la carrera de bachillerato en Informática Empresarial en el año 2006, se sumó luego el bachillerato en Turismo Ecológico en el 2007, bachillerato en Bibliotecología con énfasis en Bibliotecas Educativas en el 2008 (plan especial) y, finalmente, en el 2009 se dio la desconcentración de la carrera de bachillerato en Inglés y la licenciatura en Enfermería; esta última bajo el marco de un convenio interuniversitario entre la Universidad de Costa Rica (UCR), Universidad Estatal a Distancia (UNED) y Consejo Nacional de Rectores (CONARE). La carrera de Enfermería solo se ofertó durante los años 2009 y 2010. Cabe mencionar que carreras como Informática Empresarial y Turismo Ecológico se imparten únicamente en sedes y recintos regionales de la UCR y se siguen

ofreciendo hasta la actualidad en el Recinto de Golfito junto con las carreras de Inglés, Ciencias de la Educación Primaria y Economía Agrícola y Agronegocios.

En el año 2006, la Universidad de Costa Rica inició una estrategia para el desarrollo de una oferta académica para la Región Brunca, mediante la creación del Recinto de Golfito. A partir de entonces se han dado avances para el fortalecimiento y búsqueda de la consolidación de la presencia de esta institución en la zona sur del país.

La presencia del Recinto de Golfito en esta región —sin duda un punto de referencia dentro del desarrollo histórico de nuestro país—, por su ubicación y recursos lo convierten en un puente facilitador entre la academia y los distintos sectores de la sociedad costarricense, así como de sus intereses a corto, mediano y largo plazo. En este sentido, la proyección que tiene la UCR, mediante el accionar del Recinto, es un aspecto que debe invitar al planteamiento de propuestas reales para que la Universidad genere cambios positivos en la sociedad, particularmente en la Zona Sur del país.

MISION:

Promover las acciones de la Universidad de Costa Rica para el mejoramiento de la calidad de vida mediante la docencia, la investigación y la acción social, incentivando el desarrollo sustentable del Pacífico Sur y del país, con los principios de calidad, solidaridad, pertinencia, eficacia y equidad.

VISIÓN:

Ser una sede de la Universidad de Costa Rica líder en el Pacífico Sur que promueva la innovación y la creatividad, con una respuesta académica sostenida, pertinente, ágil y oportuna, que responda a las necesidades de un desarrollo equitativo e inclusivo local, vinculado a la acción social y la investigación, que ratifique el compromiso institucional con la regionalización, fortaleciendo las alianzas estratégicas.

Análisis del tráfico de la red de datos del Recinto de Golfito

Actualmente, el tráfico de la red de datos del Recinto Golfito muestra un mayor uso debido al aumento de la población estudiantil y docente, comprometiendo el ancho de banda en contenido no prioritario para las labores de docencia y administrativas, además de la creación de nuevos puestos administrativos que generan consumo y producción de contenido casi desproporcionado. Por ello, es importante gestionar la información en tiempo real y así usarla como punto de apoyo en la toma de decisiones relacionadas a la administración de sistemas informáticos. Se presenta entonces la necesidad de analizar datos de forma inteligente, los cuales puedan brindar conocimiento útil para la toma de decisiones.

Tenelanda y Vallejo (2012) exponen que el análisis o entendimiento de los datos "comprende la recolección inicial de datos, en orden a que sea posible establecer un primer contacto con el problema, identificando la calidad de los datos y estableciendo las relaciones más evidentes que permitan establecer las primeras hipótesis" (p. 52).

Santos *et al.* (2006) destacan la importancia del análisis de datos y su exploración:

> Es conocida la frase "los datos en bruto raramente son beneficiosos directamente". Su verdadero valor se basa en: (a) la habilidad para extraer información útil la toma de decisiones o la exploración, y (b) la comprensión del fenómeno gobernante en la fuente de datos. En muchos dominios, el análisis de datos fue tradicionalmente un proceso manual. Uno o más analistas familiarizados con los datos, con la ayuda de técnicas estadísticas, proporcionaban resúmenes y generaban informes. (p. 12).

Para el proceso de un análisis exhaustivo de los datos se destacan técnicas y herramientas aplicadas en la minería de datos, herramientas de graficado de la información, sistemas de medición de patrones con base en políticas lógicas ya creadas con anticipación, entre otros.

La transformación de datos muy poco legibles a información clara y concisa, para los administradores de redes y directivos de las organizaciones es clave, y punto

de partida en toda organización. Pero esto se logra por medio de la estadística aplicada en el proceso de exploración.

Administrador de Recursos Informáticos Desconcentrados (RID)

En la UCR todo el soporte y regulación de los recursos informáticos se encuentra bajo las labores del Centro de Informática (CI), que es:

> Es una oficina administrativa coadyuvante de la Rectoría y apoyo técnico del Comité Gerencial de Informática en el gobierno de las tecnologías de la información y comunicación, funciona como instancia estratégica, asesora, técnica y de servicio, dedicada a las mejores prácticas para asegurar que la información y tecnología están acordes y soportan los objetivos de la Institución hacia una posición de vanguardia y excelencia. Estará organizado en unidades y áreas agrupadas por su afinidad en divisiones. Depende directamente del Rector o Rectora. (2012, p. 1).

Además, en todas las sedes y recintos de la institución se cuenta con personal administrativo que gestiona los procesos de soporte, mantenimiento e implementación de los recursos informáticos. Según el CI:

> El personal designado como Administrador de Recursos Informáticos Desconcentrados, es el encargado de la gestión y monitoreo de la plataforma de acceso, herramientas de trabajo informáticas, sistemas de telecomunicaciones y la administración del Hardware y el Software, de cada entidad institucional (unidad, centro, facultad, escuela y afines) a la que esté asignado, deberá actuar conforme a las normas de ética profesional dictadas por sus colegios profesionales, las emitidas por organismos competentes y aquellas que disponga el Centro de Informática para garantizar la buena conducta, el respeto, la integridad, la confidencialidad y la calidad profesional en los productos y servicios que brinda a los usuarios.
>
> El Administrador RID, se regirá por la normativa, procesos técnicos, especificaciones de diseño y de desarrollo, relativos a tecnologías de la información y las comunicaciones, emitidas por el Centro de Informática; sin

embargo, dependen jerárquicamente de manera directa de cada una de las entidades institucionales en las cuales han sido nombrados.

Los perfiles de los Administradores RID se han dividido de acuerdo a las actividades y responsabilidades que deben realizar. Puede consultarlos en los siguientes enlaces: RID1, RID2, RID3.

Como referencia para la investigación, se presentan las funciones básicas de un administrador RID de acuerdo con su perfil profesional, que engloba las funciones de un RID1 hasta el RID3, según funciones presentadas en el sitio web del CI:

- Análisis, diagnóstico y reparación de fallas o problemas de navegación por la red.
- Diagnóstico y resolución de problemas de bases de datos, aplicaciones y sistemas de información.
- Diseño, configuración y gestión de las bases de datos propias y compartidas.
- Diseñar y guiar la implementación de planes de contingencia para la continuidad del servicio.
- Identificar software de interés, para su potenciación, así como otros software no aptos para el trabajo (afectan el desempeño del personal, de la red o del equipo), para impedir su utilización.
- Identificar la información crítica de su entidad y desarrollar planes para asegurar y respaldar dicha información.
- Coordinar las solicitudes de requerimientos de conectividad interna, y las necesidades de categorías de red, para su respectivo diseño e instalación.
- Coordinar el diseño y desarrollo de aplicaciones y sistemas usuarios a la medida, en cada una de las entidades a las que está asignado.

- Definir y monitorear reglas y directrices internas en su entidad, para el desarrollo de sistemas, la instalación de aplicaciones y la definición y desarrollo de bases de datos.

- Velar por el cumplimiento de la normativa de seguridad para el acceso a la información, en aplicaciones, bases de datos y sistemas internos.

- Promover la investigación en el campo de su competencia para estar al nivel de los avances tecnológicos en beneficio del desempeño y cumplimiento de sus labores y responsabilidades, que permita brindar el apoyo apropiado a la unidad y la institución.

- Servir de enlace con la entidad rectora universitaria en tecnología de información y telecomunicaciones, en lo que respecta a sistemas, aplicaciones y bases de datos.

- Planear, asignar, dar seguimiento y coordinar las actividades a su cargo.

- Elaborar un reporte semestral del desarrollo de las actividades y logros de su gestión.

- Coordinar con el Centro de Informática los servicios y productos necesarios para un adecuado desempeño de sus responsabilidades y la cobertura de las necesidades de la unidad a la cual está asignado.

- Ejecutar las tareas y responsabilidades pertinentes al administrador de RID II (técnico avanzado), en caso de ausencia temporal o permanente de este perfil en la entidad organizacional.

- Coordinar o supervisar personal técnico o asistencial, en los casos en que esto sea necesario, especialmente en lo que respecta a administradores de RID I y II.

Como queda establecido, el RID debe desarrollar labores de soporte, mantenimiento, gestión de los activos institucionales y de la red de datos de la sede o recinto a que pertenecen; por consiguiente, es importante tener claro

cuáles herramientas y técnicas ayudan a agilizar el proceso de gestión de la información. Para eso es fundamental conocer los conceptos de captura, monitoreo y análisis de la información y algunas herramientas existentes; además de las leyes y directrices internacionales, gubernamentales e institucionales en privacidad y seguridad de la información.

Actualmente, el Recinto de Golfito cuenta con una oficina de Informática compuesta por un RID, donde se desarrolla cada una de las actividades antes mencionadas.

Metodología

Naturaleza del proyecto

Cualitativa

Con la implementación de este TFIA, se pretende identificar y recomendar una solución y crear una hipótesis por medio de técnicas de observación e implementación de herramientas de monitoreo y análisis de datos, con el objetivo de recomendar herramientas de tecnologías de información y comunicación para el apoyo en la toma de decisiones.

Según Martínez (2011), el enfoque cualitativo procura “interrogarse por la realidad humana social y construirla conceptualmente, guiada siempre por un interés teórico y una postura epistemológica” (p. 10).

El énfasis básico del TFIA permite estudiar aspectos sociales del entorno, en este caso la red de la organización, además de los usuarios y su conducta ante el uso de la red y también el comportamiento de la red en sí misma. Igualmente, usar la investigación por medio de la exploración y captura de información que ayude a fundamentar la importancia de implementar herramientas TIC para la captura y análisis de información.

Como mencionan Ugalde *et al.* (2013), “la investigación cualitativa tiende a ser más abierta y flexible, permitiendo el seguimiento de nuevas líneas de investigación y la recogida de datos adicionales a medida que nuevas ideas van surgiendo durante el proceso de investigación” (p. 182).

Investigación Aplicada

Como lo indica la palabra “aplicada”, se enfoca en investigar un problema específico, a partir de bases teóricas aceptadas y llevarlo a las propuestas de práctica, ejecución o aplicación de los resultados. Lozada (2014) define que “la investigación aplicada tiene por objetivo la generación de conocimiento con aplicación directa y a mediano plazo en la sociedad o en el sector productivo. Este

tipo de estudios presenta un gran valor agregado por la utilización del conocimiento que proviene de la investigación básica” (p. 5).

En este TFIA se trata de identificar las herramientas TIC para monitoreo y análisis de datos, lo cual se debe determinar por medio de la instalación y configuración, enfocándose en la búsqueda y estudio de su documentación para así poder generar recomendaciones y conclusiones en el uso de las diferentes herramientas.

Todo ello con la idea de resolver la necesidad de sistemas que apoyen en la gestión y soporte de la red de datos; además, ofrecer mayor claridad en cuanto al uso que los usuarios hacen de la red de datos local del Recinto, para así realizar una mejor toma de decisiones. Es donde la investigación aplicada será un medio para resolver problemas y conocer la realidad en la intervención de procesos a cargo de la oficina de Informática del Recinto de Golfito.

Según Vargas (2008), es “el uso del conocimiento y los resultados de investigación que da como resultado una forma rigurosa, organizada y sistemática de conocer la realidad” (p. 159).

Alcance del proyecto

Exploratorio

Debido al poco conocimiento sobre herramientas de monitoreo y análisis de datos en la oficina de Informática del Recinto de Golfito, se hace necesario realizar una identificación de herramientas para su evaluación y recomendación. La información obtenida permitirá tener una idea más clara del ámbito de estudio, desde el comportamiento del usuario hasta la reacción de la red ante su uso. En la exploración de datos podemos establecer una prioridad acorde al fin de la información.

Descriptivo

Es necesario describir el ámbito de ampliación, validez, conexiones, metadatos y su comportamiento real del tráfico de la red de datos apegado al objetivo de investigación. Este TFIA pretende ser una guía para la implementación de

herramientas de monitoreo y análisis de datos para la toma de decisiones en oficinas de otros RID.

Métodos y técnicas de recolección de información

Técnicas e instrumentos de investigación

Son la base para recaudar y analizar información obtenida por medio de los sujetos. Existen distintas herramientas para llevar a cabo este proceso.

Cuestionarios

Se realizará el desarrollo de cuestionarios para la recolección de información sobre las diferentes necesidades en herramientas para el monitoreo y análisis de datos de la red local, la misma se aplicará a los RID de otras unidades de la UCR y profesionales en el área de tecnologías de información.

Repositorio Digital

Para Duperet *et al.* (2015), “los repositorios son sistemas de información que preservan y organizan materiales científicos y académicos como apoyo a la investigación y el aprendizaje, a la vez que garantizan el acceso a la información” (p. 2).

Al contar con la facilidad de estos medios de investigación, es importante realizar una búsqueda de documentación que permita apoyar la investigación sobre herramientas TIC para la captura y análisis de datos.

Observación

La observación de la recolección de datos en el uso y configuración de herramientas para el monitoreo y análisis permitirá el acercamiento a los sujetos de investigación, conocer, describir, desarrollar la necesidad de estos, por lo que se fundamenta con estas bases y se recurre a la utilización de dicha técnica para lograr el objetivo y desarrollar un proceso claro, preciso y con bases sólidas y específicas.

Infografías y gráficos

Para efectos del desarrollo del TFIA y mayor entendimiento de la información recopilada con las herramientas de monitoreo y captura de datos, es importante graficar la información recolectada en el monitoreo; por ende, se detallan herramientas que permiten visualizar los datos para la toma de decisiones con el objetivo de apreciar el uso de la red informática de una forma clara y no precisamente en tecnicismos y así identificar escenarios, eventos futuros y de prevención

Procedimiento metodológico

Título: Modelo de automatización para el monitoreo y análisis de la red de datos local del Recinto de Golfito, Universidad de Costa Rica.			
Objetivo general: Recomendar herramientas TIC para el monitoreo y análisis de los datos de la red con el fin de mejorar la gestión de la red de datos del Recinto de Golfito.			
Objetivo específicos	Actividades - Desarrollar	Técnicas - Instrumentos	Resultado - Producto
Identificar herramientas TIC para el monitoreo y análisis de datos de la red local con el fin de conocer las opciones disponibles para su posterior análisis.	1. Investigar sobre herramientas de software libre para el monitoreo de la red en tiempo real. 2. Investigar sobre herramientas de software libre para el análisis de datos. 3. Establecer comunicación con otros RID por medio de cuestionarios.	Investigación en repositorios institucionales, en páginas web de empresas con alternativas libres dedicadas a la seguridad y análisis de información. Cuestionarios, aplicados a los diferentes RID de las sedes y recintos, dispuestos a colaborar en la	Listado de herramientas para el monitoreo y análisis de datos, donde ser muestra la bitácora de trabajo con cada una de las herramientas, datos relevantes y recomendaciones.

		investigación.	
Analizar documentación y funcionamiento de las herramientas TIC para el monitoreo y análisis de datos de la red con el fin de elegir cuáles comparar.	Estudio de documentación y manuales de las herramientas seleccionadas para la implementación. 1. Instalación y configuración de herramientas de monitoreo. 2. Instalación y configuración de herramientas de análisis de datos.	Equipo para el estudio de la documentación con conexión a Internet. 1. Instalar las herramientas TIC para pruebas básicas en el equipo de trabajo.	Selección de herramientas para el monitoreo y análisis de datos. 1. Documentación de las herramientas instaladas, y que cumplan con los objetivos de monitoreo y selección.
Comparar las herramientas TIC para el monitoreo de los datos en la red con el propósito de identificar las fortalezas y debilidades de cada una.	Instalar y configurar herramienta de monitoreo y análisis de datos. 1. Observación del comportamiento de las herramientas y analizar si se	Un servidor local que permita virtualización para la instalación y pruebas de herramientas. Equipos de cómputo en función de 1. usuarios de la red para probar el	Documentación de las herramientas instaladas, y que cumple con los objetivos de monitoreo y selección. 1. Datos sobre el uso de las herramientas en

	apega a nuestros objetivos de la investigación. Análisis de la información generada y datos estadísticos para el visto bueno de uso de las herramientas en posteriores análisis.	funcionamiento de las herramientas. 2.	el monitoreo y análisis de la red y documentación respectiva. Toma de decisiones en el uso de las herramientas de la red como medio de apoyo en la toma de decisiones.
Evaluar herramientas TIC para el monitoreo y análisis de datos con el fin de mejorar la gestión de la red de datos del Recinto de Golfito.	Generar la evaluación y recomendación de las herramientas que cumplen con el objetivo de la investigación Comunicar y promocionar la guía realizada.	Informes en línea y físicos sobre los datos generados en la selección de las herramientas. Documentación guía para la implementación de las herramientas Comunicación y promoción de la solución obtenida.	Documentación de Interés de la administración, dirección y personal de la organización. Toma de conciencia y mejora en el uso de herramientas para el monitoreo y análisis de datos, como medio de apoyo en las tomas de

			decisiones referentes al uso de la red de datos local. Compartir la información generada con colegas y personas interesadas en la aplicación de las herramientas en sus unidades a cargo, y como medio de apoyo en su gestión de las TIC.

Resultados

El contexto del desarrollo de la investigación se realizó en la Oficina de Informática del Recinto de Golfito, parte de la atención que se le hace a los requerimientos, se plantea desarrollar un investigación y puesta en práctica de herramientas de monitoreo y análisis, como forma de ayudar a la gestión de la red de datos y los servicios ofrecidos..

Para ello, se realizó un estudio de posibles herramientas que ayuden a la solución de los requerimientos y su gestión sea intuitiva y de rápido aprendizaje, primero se toma en cuanta estudios realizados en otras entidades universitarias como tesinas y artículos de tecnología; así mismo, se elaboró un cuestionario en línea “Ver anexo #2” para aplicar a los diferentes administradores RID de las Sedes y Recintos, para conocer la realidad en cuanto el conocimiento sobre herramientas de monitoreo y análisis de la red de datos, además de posibles herramientas que recomienden o necesiten aprender.

El cuestionario en línea se compartió en el foro institucional de RID y se obtuvieron 8 respuestas. De la información generada se obtiene que la mayoría de RID entrevistados, un 57.1% tiene un rango de edad de entre 30 y 34 años, un 28.6% entre los 35 y 40 años; además un 14,5% tiene una edad de 45 o más años, tal como se indica en el Gráfico 1.

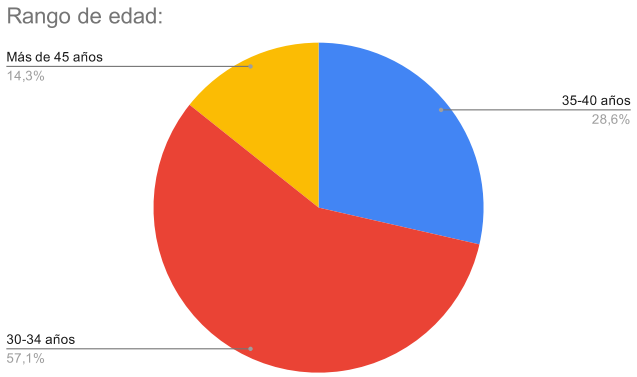


Grafico 1: Rango de edad

Un dato importante obtenido sobre los encuestados es la cantidad de años que han laborado en la institución, se puede entender que acorde al tiempo de laborar tienen mayor conocimiento de herramientas para gestionar su plataforma informática a cargo. En el Grafico 2 se muestra que un 57,1% tiene una cantidad de 6 a 10 años de laborar en la Universidad de Costa Rica, el rango de 1 a 3 años, 25 y 18 años un 14.3% cada uno; lo cual respalda lo presentado en el Grafico 1 sobre el rango de edad con mayor porcentaje entre los encuestados.

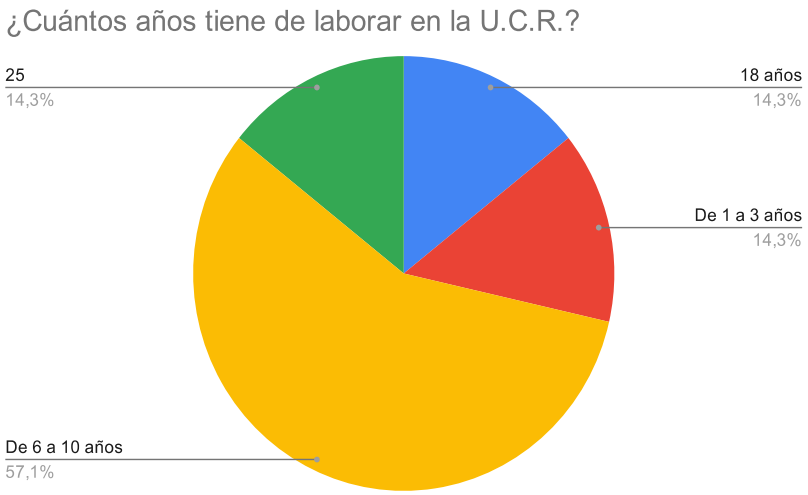


Grafico 2: Rango de años laborados de los RID que participaron del cuestionario

El 100% de los encuestados mencionó que es importante poder contar con alguna herramienta para el monitoreo y análisis de datos de la plataforma informática a su cargo, sin embargo, un 12,5% del total dijo no tener conocimiento sobre herramientas para monitoreo de datos ya sea libres o privativas. Otro 12.5% dijo sí conocer herramientas para el monitoreo y análisis de datos; sin embargo, son de la plataforma instalada por el Centro de Informática la cual brinda un acceso mínimo, con limitaciones para gestionar toda la plataforma. Además, se menciona Wireshark el cual es ampliamente usado en oficinas de distintos RID.

En el Grafico 3 se presentan los resultados obtenidos con respecto al método de aprendizaje, el 50% de los encuestados mencionan que han tenido acceso y han

aprendido a usar herramientas por el medio del autoaprendizaje, un 33,3% por medio de capacitación y un 16,7% son herramientas instaladas por el centro informática pero con la limitante de uso.

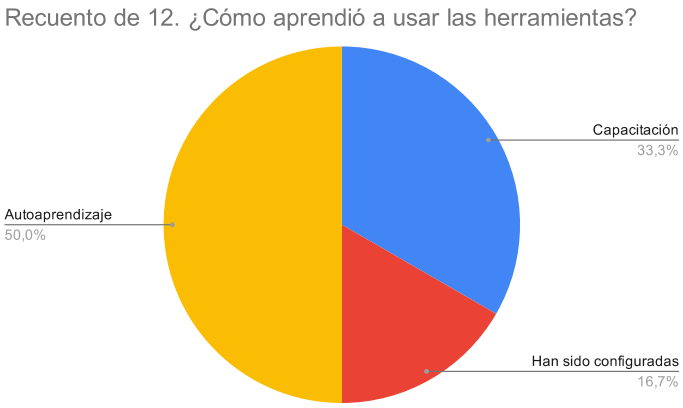


Grafico 3: Método de aprendizaje.

Para fortalecer el conocimiento de herramientas de monitoreo y análisis se consultó sobre la importancia de capacitación de instalación y configuración de herramientas libres para el monitoreo y análisis de la red de datos local, a ello el 100% de los participantes de la encuesta exclamó que es de suma importancia poder contar con capacitación y guía.

Los resultados de la aplicación de la encuesta mostró que los diferentes RID de las unidades, sedes y recintos de la UCR necesitan conocer más sobre herramientas para gestionar sus plataformas informáticas. Es justamente en eso donde el software libre ayuda a tener herramientas que son de gran utilidad y fácil acceso; sin embargo, tienen una curva de aprendizaje que se puede resolver con capacitaciones. Esto genera una gran necesidad de poder gestionar la estructura informática con el fin de mejorar la seguridad.

Como resultado de la encuesta aplicada y el análisis de la investigación de herramientas de monitoreo y análisis se ha generado un listado. El total de las herramientas en la lista que se muestra en la Tabla 1 las cuales se clasifican en una posible categoria de uso; además son opciones libres, con un costo de

implementación por licenciamientos nulo o mínimo, seleccionadas de manera que la curva de aprendizaje e implementación sea sencillo. :

Captura de datos red local	Monitoreo de equipos.	Análisis e interpretación de datos.
Wireshark	Telegraf	Networkminer.
Nmap	InfluxDB	Grafana
Ntopng.		Rapidminer
EtherApe		

Tabla 1: Listado de herramientas clasificadas por categoría

Cada una de las herramientas anteriormente mencionadas fueron probadas y se obtuvo la siguiente información.

La instalación y configuración de todas la herramientas se realizó en diferentes equipos y plataformas los cuales son:

- Un sistema operativo Debian 9 de 64 bits Núcleo Linux 4.9.0-9-amd64 x86_64, el quipo donde se realizó la instalación es una computadora de escritorio marca HP modelo ProDesk con un Intel® Core™ i5-6600 CPU @ 3.30GHz × 4 y 16 gigas de RAM.
- Un equipo con Windows 10 de 64 bits marca Lenovo ThinkPad T480 con Intel® Core™ i7-8550U CPU @ 1.80GHz 1.99GHz y 16 gigas de RAM.
- Un servidor de virtualización con Proxmox 5.4 en el cual se crea una máquina virtual con el sistema operativo Debian 9

Wireshark

Funcionalidad:

Esta herramienta fue desarrollada por Gerald Combs bajo la modalidad open-source. Está disponible para plataformas Windows y Unix y permite ser usada como herramienta principal de monitoreo, o bien como punto de partida para otras herramientas, para un análisis más profundo.

Es un analizador de protocolos de red, el cual permite observar lo que sucede en la red de forma detallada. Esta herramienta es ampliamente usada para estudio y resolución de problemas en redes de datos, soportando más de 1100 protocolos. Se puede utilizar en modo consola, con una interfaz gráfica intuitiva y de fácil uso.

Resultados:

Se realizó una captura general del tráfico de la red en horario de oficina el cual comprende de las 8am a 5pm. En la puesta en marcha de la aplicación se observa una facilidad de uso e interpretación sencilla de los datos capturados.

Parte de la configuración inicial en Wireshark es activar la casilla en modo promiscuo, el cual permite capturar el tráfico de red en su totalidad.

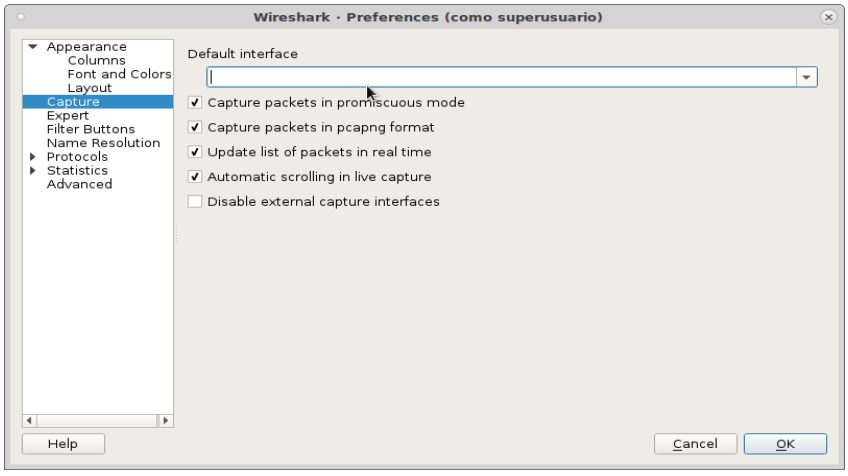


Figura 1: Activación con modo promiscuo, configuración inicial.

Seguido en el menú de captura se genera un listado de las interfaces de red por las cuales se captura el tráfico de la red- Para efecto de esta revisión se seleccionó la eno1, la cual está conectada y configurada a la red principal de datos del recinto.

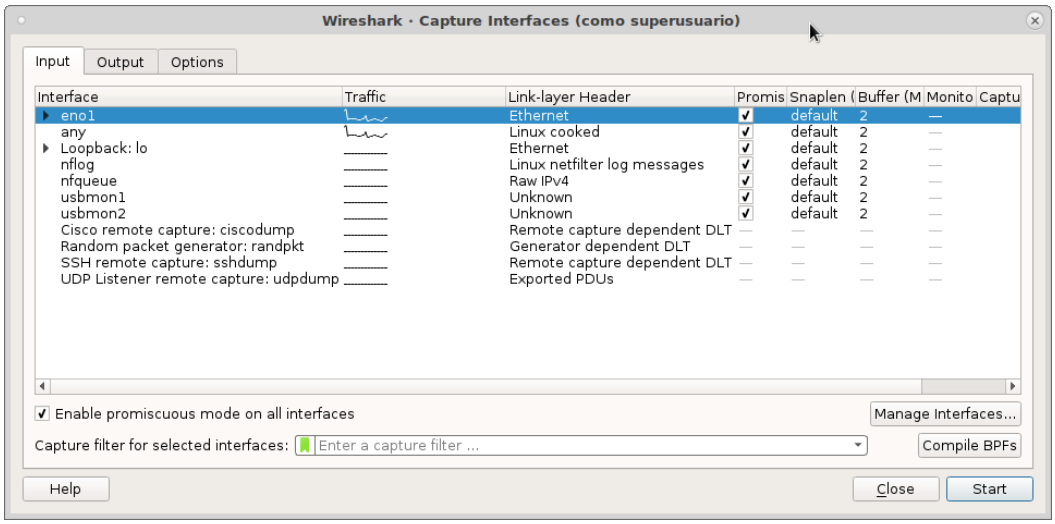


Figura 2: Listado interfaz de red

Al dar clic sobre el botón “Iniciar” la herramienta muestra la interfaz principal de Wireshark, la cual se divide en tres paneles:

- Paquetes: que a su vez se divide en filas y columnas, las filas representan los paquetes capturados de forma secuencial y las columnas información referente a los paquetes capturados
- Detalles del paquete: en el que se muestra información del paquete seleccionado y su estructura
- Bytes: que se compone de desplazamiento del paquete, los datos en hexadecimal y la representación ASCII del paquete.

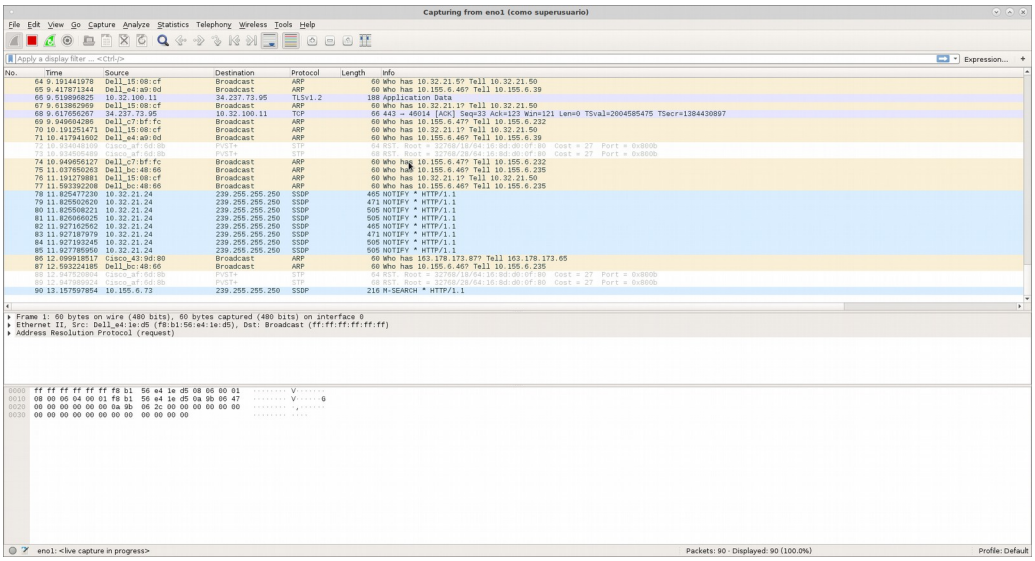


Figura 3: Interfaz principal de Wireshark

Wireshark permite gran cantidad de funcionalidades a partir de una captura de paquetes para mostrar en tiempo real lo que sucede en la red de datos local, aplicando filtros al tráfico capturado. Por ejemplo, aplicar un filtro por protocolo como en la Figura #3 en la que se muestra un filtrado del protocolo ARP.

Para efectos de la prueba de la herramienta la configuración utilizada es simple. Si bien es cierto es una herramienta muy extensa que permite una cantidad de capturas sobre la red de datos, pero con al hacer una captura sencilla se logra observar información relevante de la información que se mueve en la red, permitiendo poder anticipar ataques sobre la red y, además, entender de forma detallada muchos de los comportamientos del usuario.

Otra facilidad que brinda la herramienta es el módulo de estadísticas en el que se muestra información relevante del tráfico de red capturado. Este apartado brindó datos de los diferentes equipos presentes, además estadísticas del tráfico tcp/ip en general.

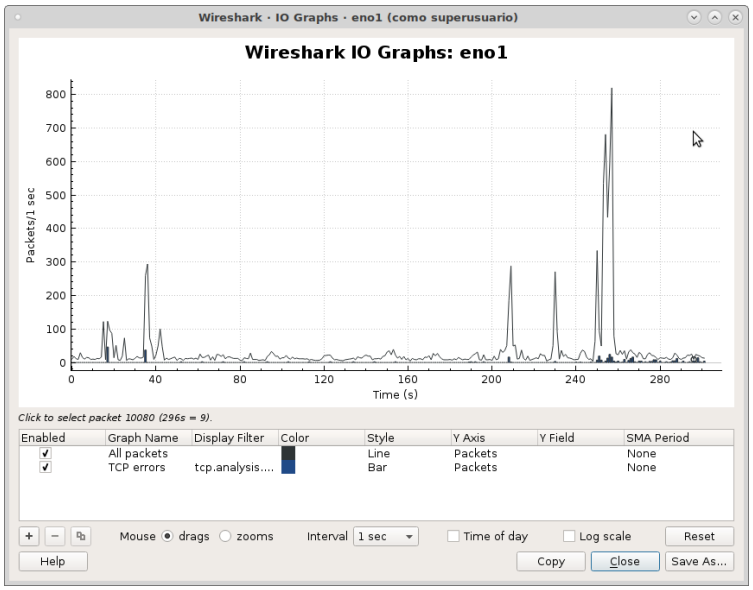


Figura 4: Gráficas del trafico de entrada y salida.

En la Figura #4 se logra observar una gráfica del tráfico entrante y saliente de la captura realizada, permite personalizar varias opciones para su uso.

Al finalizar la captura de datos la herramienta permite guardar las tramas completas en un archivo .pcap, el cual puede ser leído y analizado por otras herramientas para un análisis más claro y completo si fuese necesario.

Ventajas:

- Es multiplaforma.
- Permite la captura en tiempo real de los paquetes de datos transmitidos en la red de datos local.
- Permite la captura de más de 1100 protocolos.
- Cuenta con una interfaz gráfica de fácil uso.
- Facilita el filtrado de paquetes.
- Importar y exportar la información capturada para un posterior análisis en otras herramientas.
- Módulo de estadísticas para un análisis rápido.
- Muestra las capturas por color acorde a los protocolos capturados.

Desventajas:

- Se requiere de una curva de aprendizaje para lograr una interpretación la información capturada.
- Es necesario contar con conocimientos en protocolos y plataformas existentes en la red de datos local.
- En el caso de las versiones de Linux, se debe tener permisos de súper usuario para poder hacer las capturas en la interfaz de red del equipo de cómputo.

Nmap

Funcionalidad de Nmap:

Nmap es una herramienta de software libre y código abierto que permite la exploración de redes en busca de vulnerabilidades, por medio de la exploración de direcciones ip, servicios y puertos en los objetivos predefinidos.

Resultados:

Para el uso de la herramienta Nmap se realizó por medio de la interfaz gráfica Zenmap, como se observa en la figura 1 permite ingresar la dirección IP del equipo objetivo del escaneo, se selecciona el perfil de escaneo el cual brinda las opciones de escaneo por puertos tcp, udp, escaneo de ping y ruta trazada para llegar al equipo objetivo, además como parte del escaneo nos permite observar puertos abiertos del equipo, tipología de red y descripción general del sistema operativo del equipo.

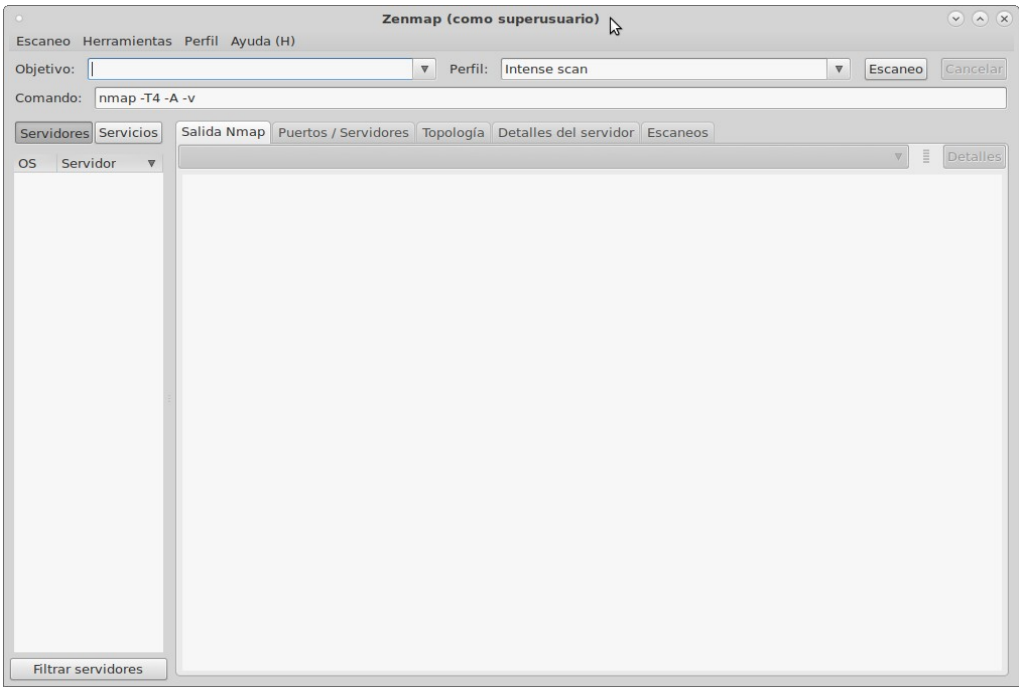


Figura 5: Interfaz principal de Nmap

Se hace un escaneo intenso a dos equipos localizados en la red del recinto, uno es un servidor y una computadora de escritorio; para el servidor se realiza un escaneo de descubrimiento de puertos TCP abiertos como se observa en la Figura #6.

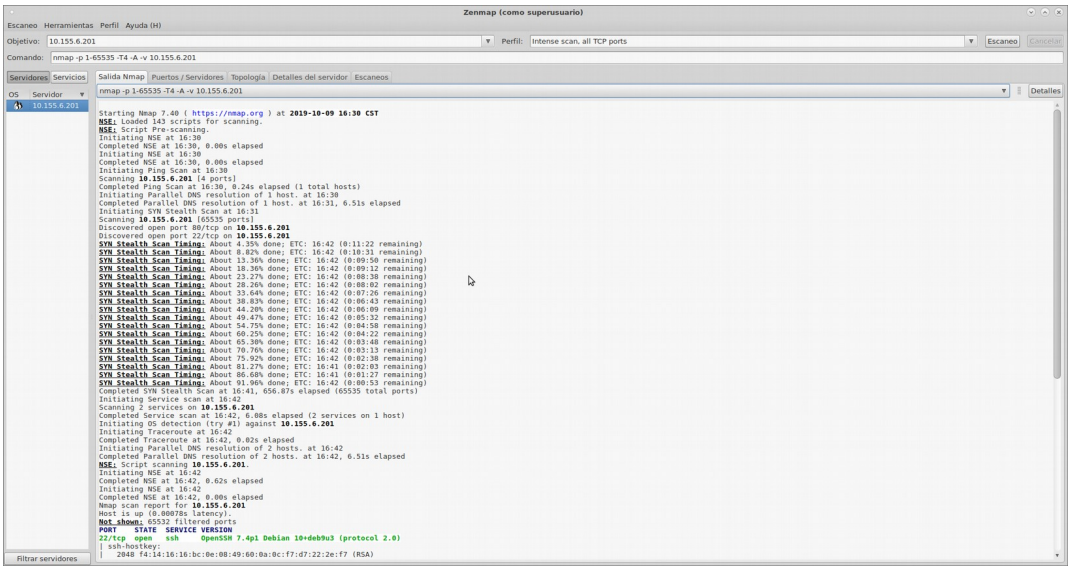


Figura 6: Descubrimiento de puertos habilitados en servidor web.

Una de las ventajas de usar herramientas como Nmap y su interfaz gráfica zen, la cual permite observar los resultados de una forma más clara y detallada, esto gracias al uso de pestañas la cual emite la información acorde a la requerido, las pestañas presentes en la herramienta son; salida Nmap la cual muestra un resumen general del escaneo realizado, como pestaña principal muestra toda la información durante y después del proceso del escáner.

La pestaña de puertos y servidores muestra el listado de puertos abiertos o en si habilitados en el equipo escaneado, es más en detalle y vista rápida; en la pestaña de topología muestra de forma gráfica el mapa de la ruta a seguir desde el equipo donde se originó el escaneo hasta el destino que es el equipo escaneado esto ayuda a distinguir de forma fácil los diferentes saltos que hay en la ruta del escaneo; además tiene una pestaña de detalles del servidor el cual divide el resultado sobre información más detallada del equipo que se le realizó el escaneo, detalles como estado del servidor, direcciones IP, versiones del sistema operativo, incluso si hay algún firewall en el medio detalla dicha información.

El uso de Nmap es muy sencillo pero potente, muchas de los ataques y defensas se originan de herramientas de este tipo, las cuales nos muestra la información detallada pero sencilla del equipo destino, Nmap también se puede usar por medio de consola la cual es por medio de la ejecución de comandos y parámetros se logra recopilar la información requerida, algunos ejemplos de comandos por consola son:

- $ nmap -sP dirección subred/mascara: nos permite mostrar las direcciones IP activas en una subred.
- $ nmap dirección subred/mascara: verifica todos los puertos abiertos en una subred específica, importante para conocer nuestras vulnerabilidades.

- $ nmap -sS -sU -PN -p 1-65535 dirección ip: busca todos los puertos abiertos en un rango especifico en el equipo asignado por la dirección ip.

- $ nmap -T4 -F dirección ip: exploración rápida en el equipo asignado con la dirección ip.

- $ nmap -iL nombre.txt: permite escanear todas las direcciones y nombres de equipos en listados en el archivo txt.

- $ nmap –iflist: lista las interfaz de red a detalle del equipo que contiene instalado Nmap

El uso de Nmap puede ser muy extenso, pero a la vez práctico para cualquier exploración de la red de datos de uso de hogar así como de pequeñas y grandes empresas.

Ventajas de Nmap:

- Es una herramienta multiplataforma se puede usar casi que en el cualquier sistema operativo del mercado tales como Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, etc.
- Es es de fácil uso lo cual permite un aprendizaje corto, pero cien por ciento funcional.
- Se centra mucha documentación sostenida por una comunidad en base a la herramienta.
- Es una herramienta flexible permitiendo el uso en modo consola o bien por interfaz gráfica.
- Se contempla varias herramientas de monitoreo y exploración en ella misma.

Desventajas:

- Se requiere tener algún conocimiento de redes para su ejecución, especial para administradores de sistemas y atacantes informáticos.

- Entre más grande es el escaneo más dura su ejecución y cuentan factores como lactancia de la red y recursos con que cuenta el computador que ejecuta Nmap.

EtherApe.

Funcionalidad de EtherApe:

Es una herramienta de monitoreo de la red de forma gráfica, permite la visualización de protocolos por color, muestra la actividad de la red en 3 modos distintos en modo IP, nombre del host y trafico TCP, además, proporciona la lectura de trafico de red en tiempo real y por medio de un archivo.

Algunos de los protocolos soportados según el sitio web oficial de EtherApe son: ETH_II, 802.2, 803.3, IP, IPv6, ARP, X25L3, REVARP, ATALK, AARP, IPX, VINES, TRAIN, LOOP, VLAN, ICMP, IGMP, GGP, IPIP, TCP, EGP, PUP, UDP, IDP, TP, ROUTING, RSVP, GRE, ESP, AH, EON, VINES, EIGRP, OSPF, ENCAP, PIM, IPCOMP, VRRP; and most TCP and UDP services, like TELNET, FTP, HTTP, POP3, NNTP, NETBIOS, IRC, DOMAIN, SNMP, etc.
Actividad realizada con Rapidminer:

Experiencia con EtherApe:

Se realizó la instalación de EtherApe la cual solo está disponible para sistemas Linux y tipo UNIX, su instalación es sencilla al ejecutar su código fuente desde modo consola, para ejecutar la aplicación es importante tener permisos de usuario administrador. EtherApe es de fácil instalación y puesta en marcha, en la figura siguiente se puede apreciar en su ejecución inicial.

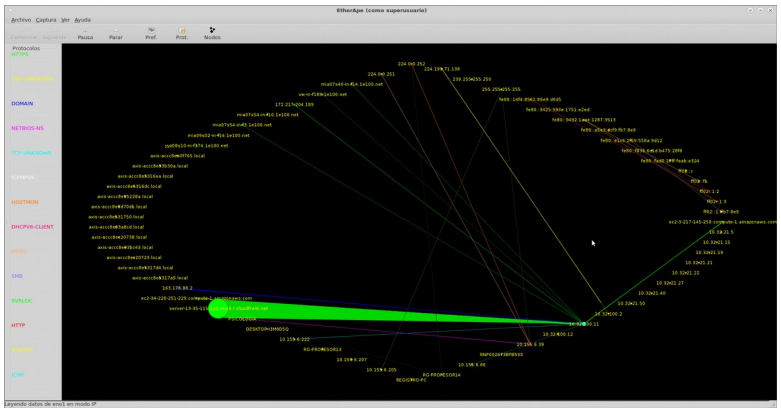
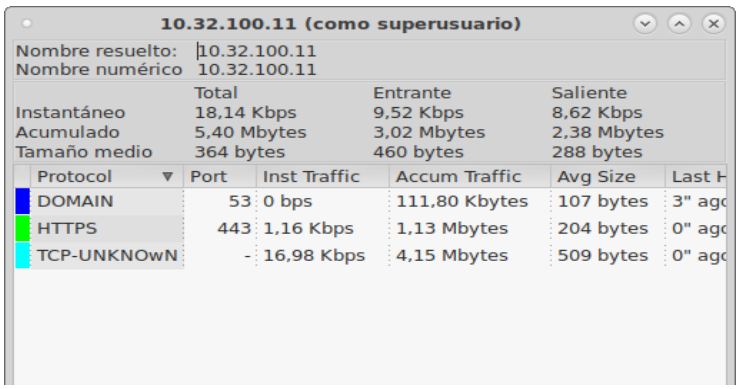


Figura 7: Ejecución inicial de EtherApe

Como se observa en la Figura #7 en el panel central muestra gráficamente el tráfico de la red de datos en tiempo real, el punto de partida de la captura es el equipo local donde se ejecuta, se puede observar la direcciones IP de origen del tráfico y las de destinos, aclarar que soporta ipv4 e ipv6; el color de las línea es acorde al protocolo capturado en donde al extremo izquierdo se puede observar los protocolos en acción con color.

Al dar clic sobre alguno de los nodos de la captura se puede observar datos del tráfico de red generado por el mismo, como se muestra en la Figura #8.



Figura

EtherApe tiene varias funcionalidades como mostrar el listado de los equipos que están interactuando en la red así como estadísticas por protocolos usados en la red, todo ello en tiempo real o bien desde la captura de un archivo generado por otras herramientas como Wireshark.

En el siguiente ejemplo de captura Figura #9, se observa como un equipo origen hace miles de solicitudes de conexión a otro equipo destino y se aprecia gráficamente como genera más carga en la red de datos.

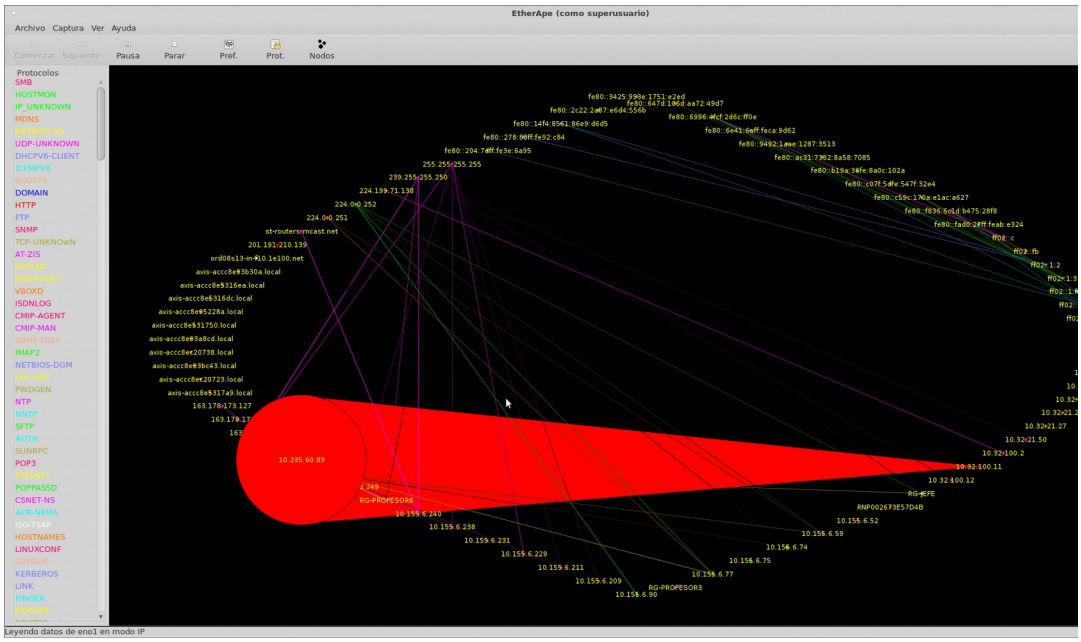


Figura 9: Captura en tiempo real.

Ventajas:

- Es de fácil instalación e implementación.
- Es una herramienta opensource.
- Observación de tráfico gráficamente.
- Permite exportar las capturas para posterior estudio y análisis.
- No consume muchos recursos del computador para su ejecución.
- Soporta más de 50 protocolos de red para su captura, su mayoría conocidos y usados diariamente.

- Una comunidad activa para soporte.

Desventajas:

- No es multiplataforma, soportada en sistemas operativos Linux y Unix
- Su funcionalidad más fuerte es observar el tráfico del equipo donde se instaló EtherApe y su conexiones para el exterior

Ntopng

Funcionalidad:

Ntop es una herramienta que permite monitorear equipos y redes en tiempo real, su interfaz de administración es vía web y se puede acceder local y remotamente a las diferentes funcionalidades, que parten desde observación del tráfico de red, protocolos, puertos, lista de equipos conectados a la red y aplicaciones en iteración.

Resultados:

Para la instalación de la herramienta de Ntop y su interfaz Ntopng se realizó por medio de la consola al ejecutar el comando “apt install ntopng”, después de su instalación se puede acceder vía web a la dirección http://localhost:3000 seguido se accede el usuario admin y contraseña admin por defecto, como se observa en la Figura #10 página principal donde se ve el monitoreo en tiempo real e histórica de la red de datos.

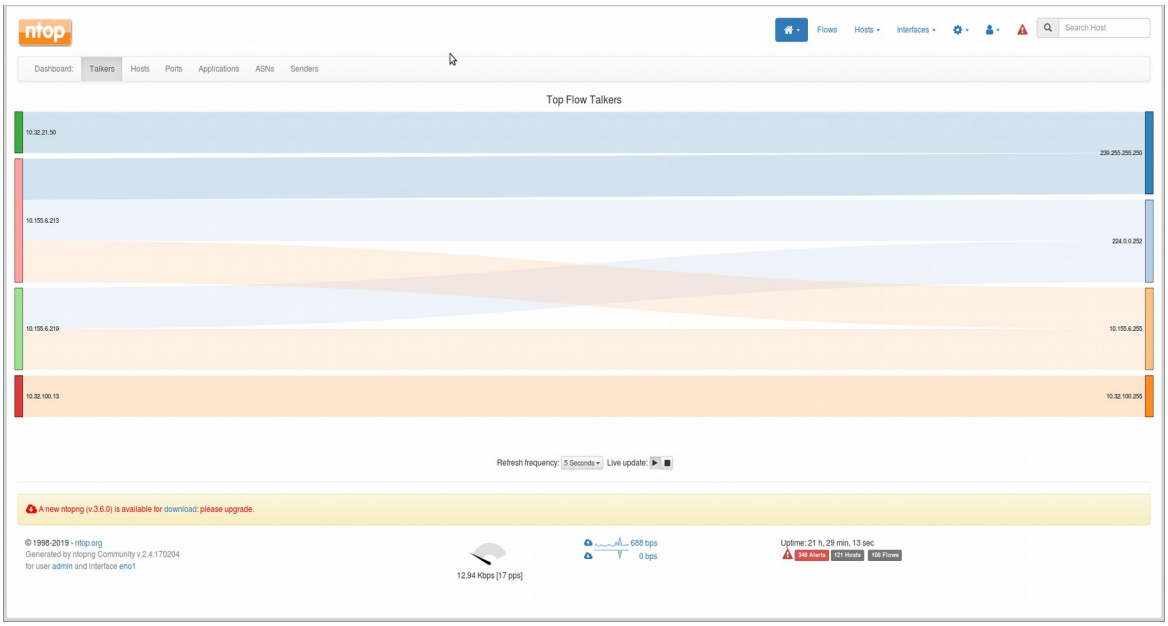


Figura 10: Pagina principal, ejecución de Ntopng

El uso de la herramienta Ntopng garantiza poco consumo de recurso dentro del computador que lo alberga, desde el monitoreo hasta la información detallada es de forma segura.

Caracteristicas importantes, que permiten a Ntopng ser una herramienta de monitoreo de nueva generación y fácil de implementar.

- Contiene una extensa lista de protocolos como ARP, ICMP, Decnet, DLC, IPX, Netbios, TCP, UDP entro otros,
- Monitoreo del tráfico por los equipos que están involucrados en el funcionamiento de la red.
- Clasificación del tráfico de la red por direcciones IP.
- Contiene Geolocalización.
- Estadística del tráfico de la red por medio de html5.
- Sistema de alertas en la captura de datos de red, principalmente por host.

Ventajas:

- Es una herramienta multiplataforma y su interfaz web es compatible para uso local como remoto.
- Contiene una configuración inicial básica.
- Informes de red históricas.
- Ordenación de trafico de red por Sistemas autónomos, puerto, dirección IP y rendimiento.
- Rendimiento en vivo de la red, los bytes y paquetes transmitidos.

Desventajas:

- Se requiere tener algún conocimiento de redes para su ejecución, especial para administradores de sistemas y atacantes informáticos.
- La versión gratis para la comunidad no contiene todas las funcionalidades, lo cual la versión para empresas si, pero es de pago.

Dashboard con InfluxDB, Telegraf y Grafana.

Funcionalidad:

InfluxDB: Es una base de datos de series de tiempo, la cual almacena cantidades de información y configurable para mejorar su rendimiento.

Chronograf: Es una interfaz de usuario y administrativa vía web para InfluxDB, entre sus funcionalidades permite la generación de gráficos de los equipos administrados por InfluxDB.

Telegraf: Es un archivo de configuración el cual permite recolectar datos de sensores como CPU, RAM, DDy servicios del equipo donde fue instalado, asi mismo enviar estos datos a InfluxDB.

Grafana: Es una herramienta para la visualización de datos en tiempo real, toma los datos de bases de datos y permite generar graficas acorde a la necesidad de

cada administrador de sistemas. Es una herramienta software libre bajo la licencia apache 2.0.

Actividad realizada con InfluxDB, Telegraf y Grafana:

Experiencia:

Para efectos de la practica realizada no se mostrara el proceso de instalación el cual puede variar según la plataforma de trabajo del usuario, pero sí es importante mencionar que todos estos sistemas son multiplaforma, en el caso de influxDB es tiene instalador para sistemas basados en linux y en mac, para Windows no. En el caso de Telegraf si es multiplataforma funciona en sistemas Linux, MacOS, Windows y Docker. La herramienta Grafana es instalable en Linux, MacOS, Windows, Docker y arm.

A continuación, se muestra en la Figura #11 de la interacción propuesta cliente-servidor para Telegraf, InfluxDB y Grafana.

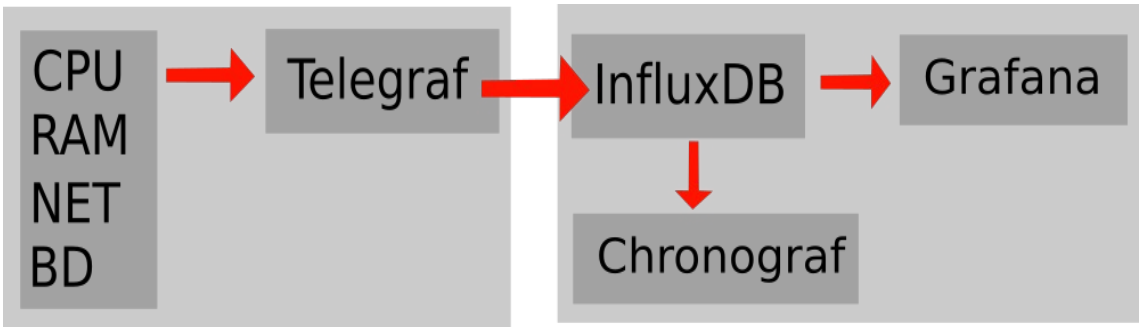


Figura 11: Propuesta de interacción cliente-servidor,, monitoreo equipos en red.

Para la instalación y configuración de InfluzDB en la maquina virtual se agregan los repositorios del InfluxDB el cual se hace modo consola, seguido a instalación del software y su interfaz grafica Chronograf. En la figura #12 se observa el sistema virtualización Proxmox y la maquina virtual con Debian 9 en ejecución.

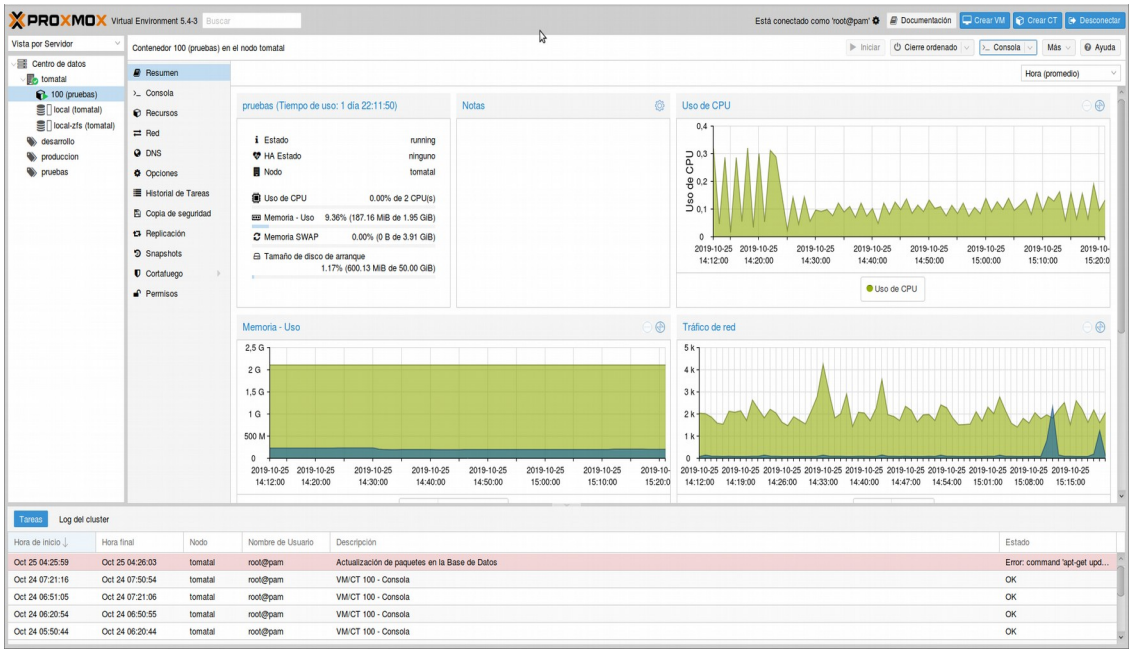


Figura 12: Maquina virtual en Proxmox

Chronograf brinda una interfaz intuitiva, la cual es sencilla de usar. Los bloques importantes son un panel de control, un listado de host, dashboard de monitoreo y un apartado para crear alertas en caso necesario. La Instalación y configuración de InfluxDB y Chronograf (interfez web para la administración de la base de datos) en debian 9, ver la Figura #13.

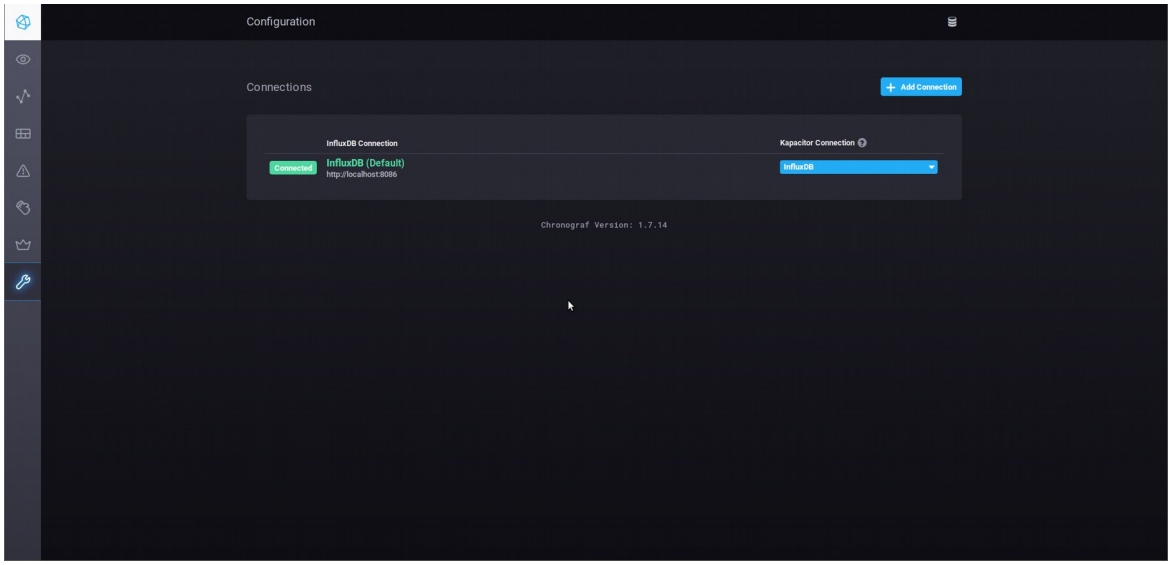


Figura 13: Conexión de Chronograf con InfluxDB.

Una vez instalado y configurada la bases de datos, la cual resguarda los datos en crudo de los equipos monitoreados, los siguiente es instalar y configurar Telegraf el cual se hace desde los equipos clientes para que envié la información a monitorear. Es un archivo de configuración al cual se le proporciona la ruta y la información de cuáles datos se deben enviar de los equipos monitoreados. Como se observa en la Figura #14 la estadística generada desde Chronograf de la computadora portátil configurada con Telegraf.

Estadística equipo cliente configurado con Telegraf.

Con la estadística generada sería suficiente para un monitoreo de los equipos desde computadoras de usuarios y servidores. Sin embargo, la gestión de las gráficas proporcionadas por Chronograf limitan su personalización y gestión, por lo cual para fortalecer el sistema de monitoreo de equipos en tiempo real e interpretación de la información se instala Grafana.

Grafana permite agregar una cantidad de orígenesde datos importante, la cual son de la mayoría de bases de datos del mercado para monitoreo y SQL, esto permite poder conectar el sistema InfluxDB y Grafana para la solución propuesta.

Para la creación de las gráficas de los equipos monitoreados, primero se selecciona el origen de datos ya configurado el cual es InfluxDB, seguido el equipo al cual se le quiere crear las gráficas de monitoreo, como se observa el Figura #15 Grafana permite crear un cantidad de graficas acorde a nuestra necesidades se selecciona al gusto y requerimiento, seguido del tipo de dato a monitorear si es la CPU, la RAM, disco duro, procesos y servicios en general del equipo cliente, así mismo brinda la posibilidad de crear alertas y tiempos de sincronización del monitoreo

Figura 15: Graficas disponibles en Grafana

Grafana es altamente modificable a las necesidades del usuario, muy fácil de entender y aprender, además muy fiable para monitoreos de organizaciones pequeñas y grandes.

Figura 16: Panel de monitoreo en Grafana.

El usar sistemas de monitoreo de los equipos de prioridad para los servicios de red y aplicaciones a los usuarios es de suma importancia debido que si un equipo sea virtual o físico se daña o sufre algún altercado se ve perjudicada la disponibilidad de la institución.

Ventajas:

- Es multiplataforma tanto para Windows, MacOs, linux, docker y arm.
- Es ampliamente utilizada en la comunidad internacional y empresarial, lo cual brinda un buen respaldo de su calidad y funcionalidad.
- Las visualizaciones se obtienen sin mucho esfuerzo.
- Conectividad con la mayoría bases de datos actuales como orígenes de datos para su posterior análisis.
- Monitoreo en tiempo real y con gráficas para los gustos y necesidades de los administradores de sistemas
- Permite la exportación de las gráficas en formato .svg .pdf .png y .jpg para su posterior uso y exposición.
- Es una herramienta código abierto.

Desventajas:

- Al ser un equipo cliente servidor se debe configurar dos o más equipos para su funcionalidad.
- Su instalación puede ser tediosa sino se conoce el funcionamiento de la arquitectura de la organización donde se implementa.
- Se debe contar con un servidor sea físico o virtual.
- Importante conocer algunos términos de estadística.

Rapidminer.

Funcionalidad de Rapidminer:

Es una herramienta para el análisis y minería de datos, cuenta con más de 500 técnicas de pre-procesamiento, modelado predictiva y descriptiva, métodos de prueba de modelos, visualización de datos. Una de sus mayores funcionalidades es el uso enlaces entre los operadores para la ejecución de las técnicas.

Experiencia con Rapidminer:

Para la descarga de Rapidminer se debe hacer un leve registro en el sitio web de la aplicación, es una herramienta multiplaforma soportada para Windows, Linux y MacOs, una vez descargada su instalación es sencilla y seguida por una asistente no hay forma de equivocarse.

En ejecución Rapidminer muestra un interfaz muy sencilla e intuitiva como se observa en la Figura 17 muestra una distribución por paneles de izquierda a derecha un panel de parámetros, al centro el panel de procesos donde por medio de arrastre se puede integrar operadores para este análisis, y el panel de la derecha desde donde se puede importar la fuente de datos a para posterior uso, así como el listado de operadores y técnicas que se pueden usar con la herramienta.

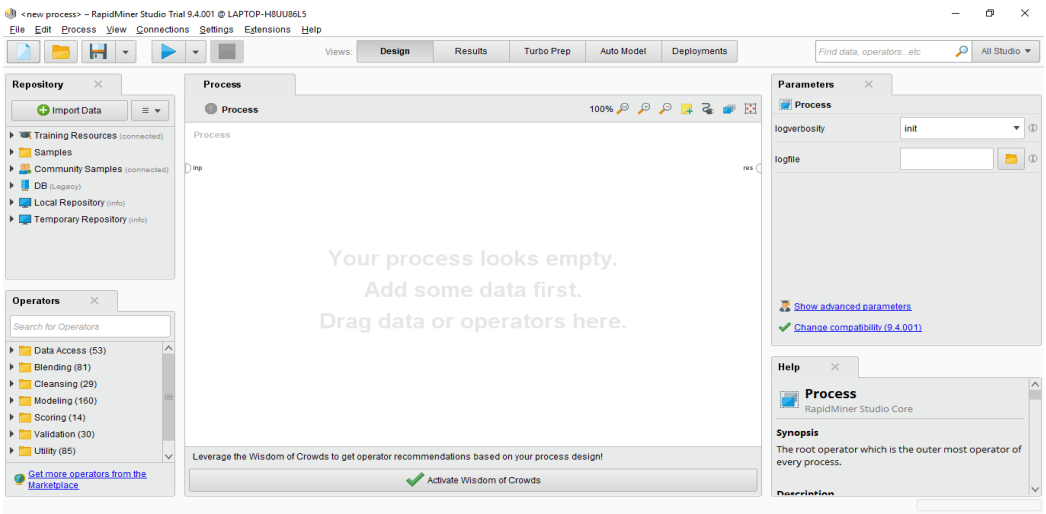


Figura 17: Entorno inicial.

Para efectos de la prueba no se hace uso de los operadores y el uso de procesos del panel central, el análisis de la información se hace por la importación de un archivo tipo .csv, el cual ha sido generado con anterioridad de una captura de datos realizada en Wireshark.

Como resultado se puede observar en la Figura 18 una tabla con los datos ordenados y agrupados.

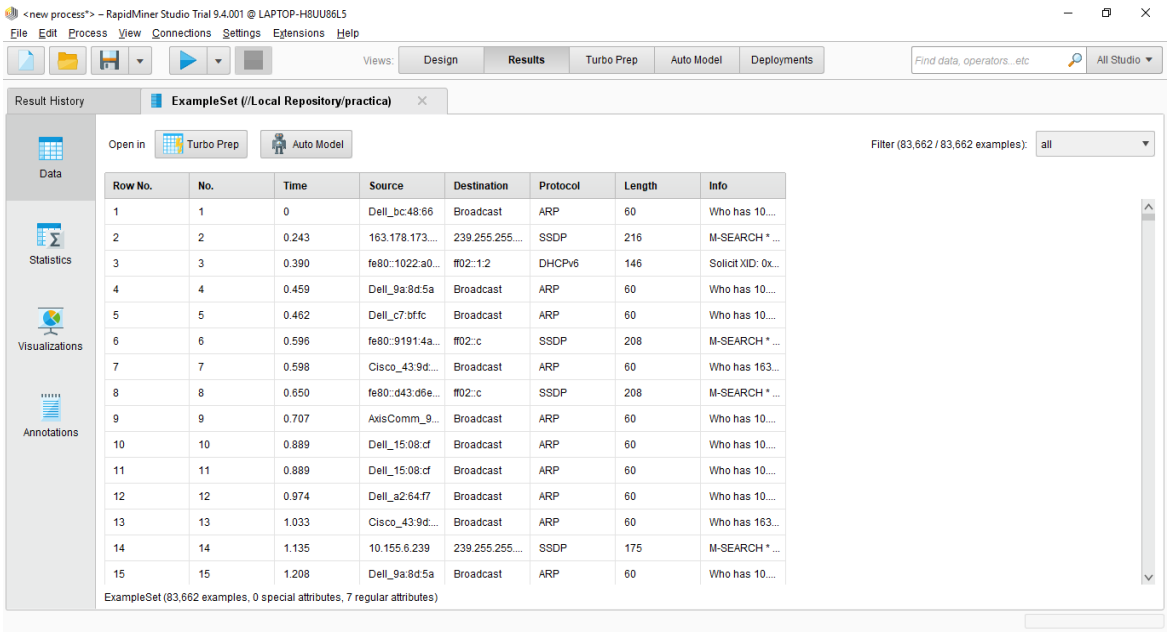


Figura 18: Datos Tabulados

Una de las mayores funcionalidades de Rapidminer es la generar estadísticas de los datos tabulados, en la Figura 19 se observa las visualización y exploración que se pueden generar en cada uno de los atributos del encabezado de la tabla de datos.

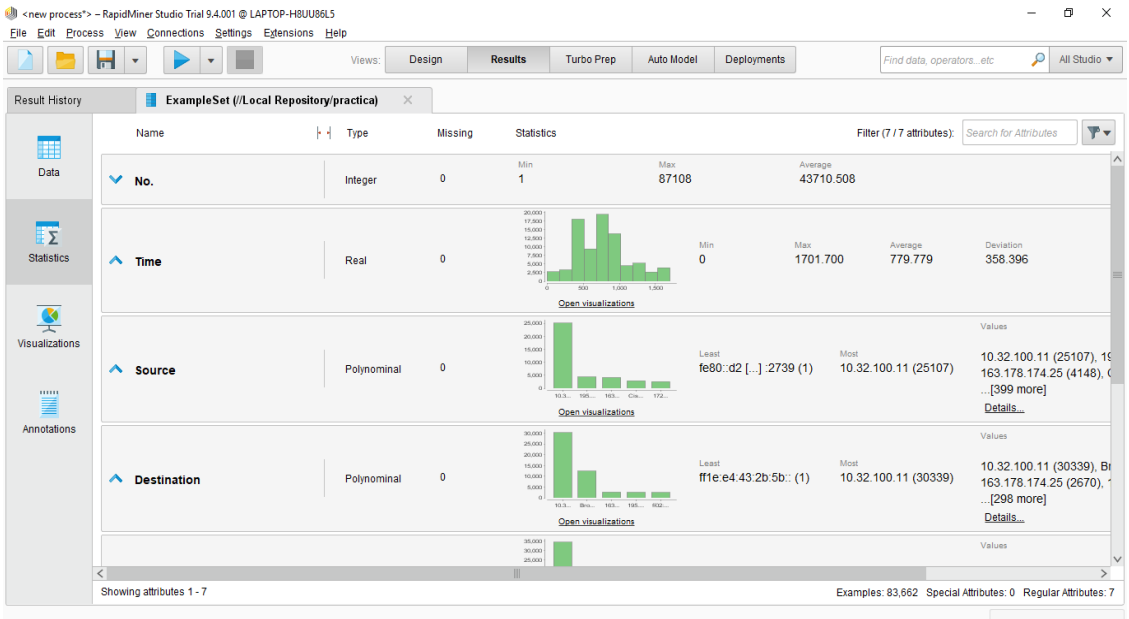


Figura 19: Estadística por atributo

Como parte de las visualizaciones que podemos hacer van desde los simples pasteles de información, visualización por medio de barras hasta gráficos como de

dispersión, tanto para gustos como para suplir de necesidades de los más exigentes. A continuación, se pueden observar un gráfico tipo pastel de los protocolos usados en la captura de datos de la red, fue realizado en Rapidminer y exportado en .svg para su posterior uso como en este caso.

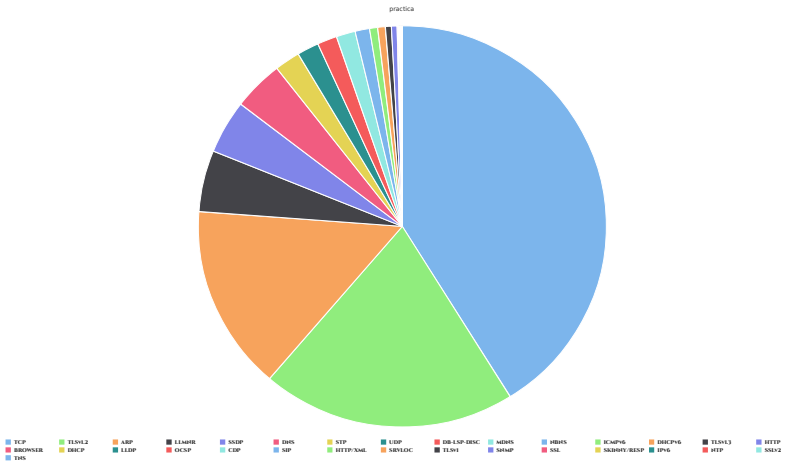


Figura 20: Grafico cantidad uso de protocolos de red, tipo pastel.

Rapidminer es una potente herramienta para la minería de datos ganadora de varios galardones desde su creación en el 2001 y considerada como la segunda herramienta para análisis y exploración del datos, usada por varias transnacionales en el campo de la tecnología, cuenta con una amplia comunidad para ayuda y soporte sobre la herramienta, una organización que brinda soluciones libres para la comunidad, estudio e investigación muy actualizada y competente, así como versiones de pago para grandes empresas que desean y pueden adquirir una solución potente y fiable.

Módulos como análisis predictivo, turbo modelado de la información y generación de procesos involucrados en la exploración se pueden hacer de forma manual al cual conlleva un curva de aprendizaje mayor, o de forma automática la cual con unos cuantos clic proporciona un análisis tabulado, con gráficas a disposición de las necesidades.

Es una Herramienta altamente recomendada, tanto para usuarios avanzados en el análisis y exploración de datos organizacionales, o bien para administradores de

red en lo cual precisa la información rápida, fiable y detallada para la generación de informes y toma de decisiones.

Ventajas:

- Es de fácil instalación e implementación.
- Es una herramienta libre bajo la licencia AGPL.
- Una herramienta multiplataforma par Windows, Linux y MacOS
- Permite exportar los análisis y gráficas en diferentes formatos como .svg, .pdf, .jpg y .png.
- Cuenta con cientos de operadores para la generación de procesos de análisis y exploración.
- Una comunidad activa para soporte.
- Se puede integrar con lenguajes como R y Python.

Desventajas:

- Si se requiere una versión empresarial tiene un costo por modulo y funcionalidades.
- Su curva de aprendizaje puede ser mayor conforme se requiere ampliar los conocimientos en estadística y minería de datos.

Networkminer

Funcionalidad de Networkminer:

Es un analizador de la red y sniffer pasivo, que permite conocer detalles de los equipos que forman parte de la captura de datos. Tiene una versión libre, lo cual permite algunas funcionalidades. La versión de profesional es más completa como sniffer, permitiendo no solo la captura de datos por archivos .pcap, sino también geolocalización, exportación de archivos y configuraciones avanzadas.

Experiencia.

Para el proceso de pruebas de la herramienta Networkminer se hace desde un sistema con Debian 9, la instalación en sistemas operativos derivados de Linux es más largo ya que se debe instalar primero el software de desarrollo Mono Develoment, el mismo para crear un entorno de ejecución con las librerías necesarias para correrlo en Linux, es una herramienta creada en principio para Windows.

En el primer acercamiento, se puede observar una herramienta muy simple lo cual permite analizar una captura ya realizada en formato .pcap, así mismo permite un monitoreo en tiempo real, ya que es un sniffer silencioso, lo cual captura tramas sin hacer enlace con los objetivos. En la Figura 21 se puede observar una captura, Networkminer clasifica la información por direcciones IP de los equipos y dispositivos, en la misma se pueden observar detalles como sistemas operativos, puertos, protocolos, dirección física entre otros.

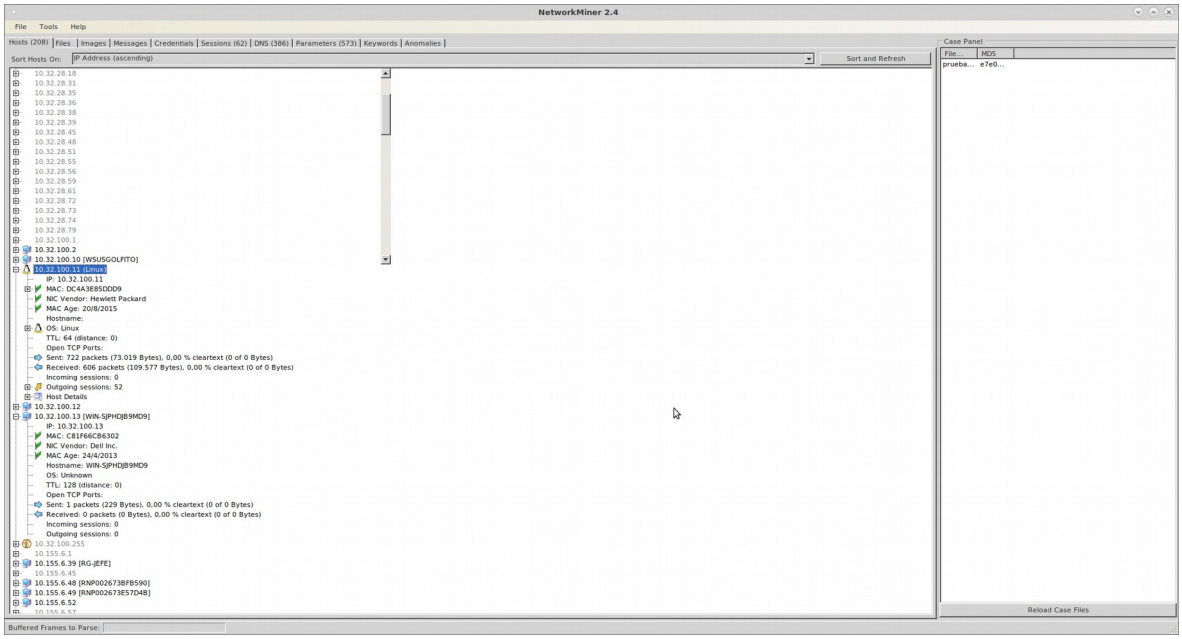


Figura 21: Networkminer interfaz

Las características principales de Networkminer versión libre según el sitio oficial:

Sniffer silencioso.
Lectura de archivos .pcap.
Soporta Ipv6
Lectura de archivos de protocolos FTP, TFTP, HTTP, SMB, SMB2, SMTP, POP3 y IMAP.
Una de sus funcionalidades es la extraer certificados de SSL encrypted traffic like HTTPS, SMTPS, IMAPS, POP3S y FTPS.
Captura de tráfico GRE, 802.1Q, PPPoE, VXLAN, OpenFlow, SOCKS, MPLS y EoMPLS.
Recibe Pcap-over-IP

Ventajas:

- Es de fácil instalación
- Es una herramienta multiplataforma, Windows y Linux
- Observación de archivos .pcap.
- No consume muchos recursos del computador para su ejecución.
- Permite la captura de imagines, certificados y registro de conexiones.
- En constante actualización y soporte.

Desventajas:

- La versión profesional contiene mayores ventajas, pero un costo elevado.
- Si se requiere exportar los datos se debe tener la versión profesional.

Recomendaciones

Luego de evaluar las ventajas y desventajas del uso de cada una de las herramientas de monitoreo y análisis de datos para la toma de decisiones probadas para esta TFIA y explicadas en el capítulo anterior, acorde a los objetivos de la UCR; se estipulan a continuación una serie de recomendaciones, las cuales abarcan desde el método de instalación hasta el uso de las herramientas en el entorno laboral y educativo.

Alternativas libres

En algunos entornos de trabajo prefieren adquirir licencias de software privativo y contratar los servicios de soporte, capacitación y garantía de las herramientas a instalar; mientras que algunos directivos prefieren la contratación de servicios de instalación, configuración y soporte de alternativas con licencias libres, para así no perjudicar la línea de trabajos de los encargados de TI. Sin embargo, con la instalación y configuración de las herramientas evaluadas se logra evidenciar que el uso de herramientas libres para los entornos organizacionales puede solventar los requerimientos de implementar un conjunto de soluciones de monitoreo y análisis de las TIC en su totalidad.

Las alternativas de software libre para el monitoreo y análisis de datos han mejorado exponencialmente con respecto a años anteriores, donde los procesos de instalación dejan de ser tediosos, muchas de las soluciones cuentan con soporte y desarrollo de empresas reconocidas en el mercado. Es importante conocer cuáles de estas son libres y de código abierto, cuáles son libres en cuanto al uso, y qué herramientas cuentan con soluciones libres pero con ciertas limitaciones en la activación de módulos, por ende, presentan una alternativa de pago más avanzada.

Lo cual si se recomienda el uso de herramientas libres o con versiones libres de las utilizadas en la práctica, ya que proporcionan lo necesario para las requeri-

mientos de la oficina y brindan resultados efectivos para un mayor interpretación de la información.

A continuación en la Tabla #2 se presenta el listado de herramientas instaladas y clasificadas como libre, de código abierto y libre pero con limitaciones de uso.

Herramienta	Libre/Código Abierto	Libre/Limitada con pago
Wireshark	X	
Nmap	X	
Networkminer		X
Ntopng		X
Grafana	X	
Telegraf	X	
InfluxDB	X	
EtherApe	X	
Rapidminer		X

Tabla 2: Listado de herramientas y su clasificación de software libre.

Equipo usado para la instalación y equipo recomendado.

La instalación y configuración de las herramientas se realizó en un equipo de cómputo de rendimiento intermedio a alto, además los sistemas operativos utilizados para el entorno de pruebas fueron Linux para escritorio y servidor y Windows en entorno de escritorio, tal como se especificó en el capítulo anterior.

En el caso de la máquina virtual creada para la ejecución de la herramienta InfluxDB y Grafana se hizo uso de un procesador de dos núcleos, 2 GB de RAM y 200 MB de Disco Duro. Es importante aclarar que conforme se use la base de datos y se aumente la cantidad de datos registrados es necesario aumentar el almacenamiento en la máquina virtual.

Como se observa para las pruebas se utilizó equipo robusto, sin embargo, no es necesario contar con equipo de elevadas prestaciones. Herramientas como Wires-

hark se ejecutan con tan solo 500 MB de RAM y un mínimo de 500 MB de almacenamiento, sin embargo, para herramienta como Rapidminer para el análisis y minería de datos, como mínimo se debe contar con un procesador Dual Core, 4 GB de RAM y 1GB de almacenamiento, pero se recomienda un procesador Quad Core , 16Gb de RAM y 100Gb de almacenamiento.

La instalación y uso de las herramientas expuestas es recomendadas utilizarlas en equipos de rendimiento intermedio a alto, sin embargo si no se posee equipos con especificaciones elevadas se puede utilizar pero con limitaciones en eficiencia.

Capacitación en el uso de la herramienta y curva de aprendizaje

En el proceso de instalación y uso de las herramientas se puede presentar retos en la implementación sobre entornos Linux, por ejemplo, tener requerimientos de dependencias y archivos de configuración a mano puede ser tedioso; como recomendación, tener un conocimiento básico en el uso de entornos Linux y de la consola es primordial, ya que se pueden resolver problemas, así como realizar la instalaciones y configuraciones de forma eficiente.

Las herramientas instaladas cuentan con una amplio respaldo por parte de organizaciones, tanto en desarrollo como en soporte; además, de una comunidad libre que brinda soporte, actualizaciones constantes y amplia documentación, con lo cual la curva de aprendizaje se vuelve menos tediosa. Al igual es importante que el usuario que realiza la instalación y uso de las herramientas tenga conocimientos en informática, principalmente en aspectos de seguridad, privacidad, sistemas operativos y redes en entornos Linux, Windows y MacOS, según su necesidad, así mismo como una correcta lectura e interpretación de datos estadísticos para la toma de decisiones.

Clasificación de herramienta conforme al uso.

El uso de herramientas de monitoreo tiene como objetivo principal el recolectar datos de los sistemas y equipos como una forma de prevenir posibles fallos de segu-

ridad y errores en el uso de las TIC dentro de la organización, por ende, se hace importante saber interpretarlos para tomar las mejores decisiones.

Con el desarrollo de las actividades en instalación y configuración de herramientas para el monitoreo y análisis de la red de datos, y equipos con servicios importantes en la red, se logró generar un listado de herramientas que puedan colaborar en el proceso de monitoreo, así como aplicaciones que proporcionan una mejor interpretación de la información capturada, para el Recinto de Golfito; tal como se muestra en al Tabla #3, las mismas se clasifican acorde al uso recomendado para su implementación, ya que herramientas que fueron clasificadas como captura de datos de la red también proporcionan módulos funcionales que permiten monitoreo y análisis de datos.

Herramienta	Captura de datos red local	Monitoreo de equipos.	Análisis e interpretación de datos.
Wireshark	X	X	X
Nmap	X		X
Networkminer.			X
Ntopng.	X	X	X
Grafana		X	X
Telegraf	X		
InfluxDB	X	X	X
EtherApe	X	X	X
Rapidminer			X

Tabla 3: Listado de herramientas y sus funciones básicas.

En las organizaciones el uso de las tecnologías de información y comunicación diariamente genera contenido en grandes medidas, tener el control de equipos de cómputo con interacción en la red local es de prioridad para garantizar la seguridad y privacidad de la información, donde el monitoreo y análisis de datos ayudan a realizar estas tareas de forma eficiente e inigualable.

Se puede tener cualquier plataforma libre o privativa para controlar las tecnologías; aunque, la seguridad y la privacidad empieza con el usuario final. Un colaborador educado y consciente de la importancia del resguardo de la información y activos institucionales, es un usuario en beneficios de los objetivos organizacionales.

Por consiguiente, una plataforma tecnológica donde un usuario educado entienda la importancia del resguardo y uso adecuado de la información, además, de un sistema que comprenda herramientas de monitoreo y análisis de datos, sin duda lograrán alinear la tecnología con la estrategia organizacional generando valor y efectividad en el transcurso del tiempo.

Bibliografía

Aguirre, E & otros. (2017). *Análisis de tráfico TCP utilizando la herramienta wireshark. Universidad Autónoma del Estado de Hidalgo.* Recuperado de https://repository.uaeh.edu.mx/revistas/index.php/huejutla/article/view/2464/2471

Apolo, A & otros. (2017). *Análisis y simulación de tráfico de la red de datos de las Fuerzas Armadas con tecnologías MPLS.* (Tesis de grado). Universidad Politécnica Saleciana, Ecuador.

Barrionuevo, M & otros. (2016). *Un enfoque para la detección de anomalías en el tráfico de red usando imágenes y técnicas de computación de alto desempeño.* Universidad Nacional de San Luis, Argentina. Recuperado de http://sedici.unlp.edu.ar/handle/10915/56370

Brenes, E & Coto, K. (2013). *Plan de comunicación e información digital para el apoyo en la*

administración de operaciones financieras pasivas, dirigido a jóvenes profesionales. (Tesis de posgrado). Universidad Estatal a Distancia, Costa Rica.

Burns, E. (2016). *Técnicas de visualización de datos, herramientas de núcleo del análisis avanzado.* Recuperado de https://searchdatacenter.techtarget.com/es/cronica/Tecnicas-de-visualizacion-de-datos- herramientas-de-nucleo-del-analisis-avanzado

Universidad de Costa Rica. (2015). *Directrices de seguridad de la información de la Universidad de Costa Rica, Resolución R-102-2015.* Centro de Informática, Costa Rica.

Chen, S. (2007). *Alcance de la legislación costarricense en materia de delitos informáticos: un análisis preliminar.* Inter Sedes. Vol. VIII. 49-67. Universidad de Costa Rica, Costa Rica.

Córdoba, J. (s,f). *La legislación costarricense y el derecho de acceso a la información pública.* Recuperado de

http://www.oas.org/es/sla/ddi/docs/acceso_informacion_base_dc_leyes_pais_cr_2.pdf

Corchado, J & Villalba, A. (s,f). *Análisis de las ciberamenazas. pp. 98-137 .*

Duperet. E & otros. (2015). Importancia de los repositorios para preservar y recuperar la información. Recuperado de http://scielo.sld.cu/pdf/san/v19n10/san141910.pdf

ESET. (2018). *ESET Security Report Latinoamerica 2018.* Recuperado de https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

Franganillo, Jorge. (2009). Gestión de información personal: Elementos, actividades e integración. Profesional De La Informacion - PROF INF. 18. 399-406. 10.3145/epi.2009.jul.06.

García, F. (2013). *Aplicación de técnicas de Minería de Datos a datos obtenidos por el Centro Andaluz de Medio Ambiente (CEAMA).* (Tesis posgrado). Universidad de Granada, España.

Gil, L. (2015). *Clasificación de tráfico de Internet mediante análisis de datos.* (Tesis de grado). Universidad Politécnica de Madrid: Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación, España Recuperado de http://oa.upm.es/38925/1/PFG_LUIS_GIL_DELGADO.pdf

Hoyos, J & Valencia, A. (2012). *El papel de las TIC en el entorno organizacional de las PYMES.* Revista TRILOGÍA No. 7, pp. 105 – 122.

Junco, G & Rabelo, S. (2018). *Los recursos de red y su monitoreo.* Revista Cubana de Informática Medica, *vol.10 no.1.* Recuperado de http://scielo.sld.cu/scielo.php? script=sci_arttext&pid=S1684-18592018000100009

Klenzi, R & Lopez, M. (2017). *Detección de ataques dos con herramientas de minería de datos.* Universidad Nacional de San Luis, Buenos Aires. Recuperado de http://sedici.unlp.edu.ar/handle/10915/61637

Martín, S. (21 de agosto de 2017). *Motorización de Sistemas Informáticos.* [blog]. Recuperado de https://blog.pandorafms.org/es/monitorizacion-de-sistemas/

Morales, N & Slusarczyk, M. (2016). *Análisis de las estrategias empresariales y de las TIC.* 3C Empresa (Edición núm. 25) Vol.5 – No 1. Recuperado de http://ojs.3ciencias.com/index.php/3c-empresa/article/view/322

Observatorio de la ciberseguridad en América Latina y el Caribe. (2016). *Informe ciberseguridad 2016, ¿Estamos preparados en América Latina y el Caribe?.* Recuperado de http://www.observatoriociberseguridad.com

Riquelme, J & otros. (2006). *Minería de datos conceptos y tendencias. Inteligencia artificial:* Revista Iberoamericana de Inteligencia Artificial, 10(29),11-18. Recuperado de https://idus.us.es/xmlui/handle/11441/43290

Sánchez, D. (2017). *Implementación de un sistema de monitoreo y protección de datos en ls red de la Facultad de Ingeniería en sistemas, electrónica e industrial*. (Tesis). Universidad Técnica de Ambato, Ecuador.

Sequera, M. (8 de marzo de 2018). *Derechos humanos y seguridad digital: una pareja perfecta*. [blog]. Recuperado de https://www.tedic.org/derechos-humanos-y-seguridad- digital-una-pareja-perfecta/

Tableau Software (2019). *Guía de visualización de datos: definición, ejemplos y recursos de aprendizaje.* [blog]. Recuperado de https://www.tableau.com/es-es/learn/articles/data- visualization

Tenelanda, G & Vallejo, D. (2012). *Minería de datos aplicada en detección de intrusos.* Ing. USBMed, Vol. 3, No. 1. Medellín, Colombia.

Vargas, Z. (2008). LA INVESTIGACIÓN APLICADA: UNA FORMA DE CONOCER

LAS REALIDADES CON EVIDENCIA CIENTÍFICA. Recuperado de https://revistas.ucr.ac.cr/index.php/educacion/article/viewFile/538/589

Anexos

Anexo # 1

Titulo.

Prueba de sistema de captura de datos Wireshark

Fecha.

Martes 4 junio.

Nombre de la herramienta.

Wireshark

Versión.

2.6

Descripción de la herramienta.

Software open source que permite interceptar el trafico en tiempo real, se permite la identificación de paquetes por direcciones ip de los equipos usados en la red, por lo general captura paquetes tcp, udp y icmp, dentro de sus utilidades más importantes es el filtrado de paquetes y en ultimas versiones permite general un pequeña estadística de los paquetes capturados.

Especificaciones técnicas de los equipos utilizados.

Procesador Intel Core i7-8550U CPU 1.80GHz 1.99GHz
RAM 16,0 GB
Tipo de sistema 64 bits

Descripción de la prueba.

- La instalación del software se realizó en horario fuera de oficina, sin embargo la ejecución y captura de paquetes se realiza dentro del horario de oficina, se considera horarios donde el uso de la red es mayor por ejemplo martes de 9am a 4pm.
- Se selecciona la interfaz de red por la cual se hará la captura.
- Como observaciones importantes se activa el modo promiscuo en la herramienta lo cual nos permitirá capturar todos los paquetes que recorren en la red local del Recinto de Golfito.

- De primera ejecución no se realiza ningún filtrado en tipos de paquetes o equipos por dirección ip, se hace una captura general del tráfico de red.
- La captura completa se guarda con el formato .pcap

Resultados.

- Uso de la interfaz de la herramienta eficientemente, lo cual se aprecia una interfaz sencilla y fluida para su utilización
- Captura de datos completa acorde al horario estipulado.
- Archivo .pcap para futuro análisis.

Titulo.

Prueba de sistema de captura de datos Wireshark

Fecha.

Miercoles 12 junio.

Nombre de la herramienta.

Wireshark

Versión.

2.6

Descripción de la herramienta.

Software open source que permite interceptar el trafico en tiempo real, se permite la identificación de paquetes por direcciones ip de los equipos usados en la red, por lo general captura paquetes tcp, udp y icmp, dentro de sus utilidades más importantes es el filtrado de paquetes y en ultimas versiones permite general un pequeña estadística de los paquetes capturados.

Especificaciones técnicas de los equipos utilizados.

Procesador Intel Core i7-8550U CPU 1.80GHz 1.99GHz
RAM 16,0 GB
Tipo de sistema 64 bits

Descripción de la prueba.

- La instalación del software se realizó en horario fuera de oficina, sin embargo la ejecución y captura de paquetes se realiza dentro del horario de oficina, se considera horarios donde el uso de la red es mayor por ejemplo martes de 9am a 4pm.
- Se selecciona la interfaz de red por la cual se hará la captura.
- Se hace una captura de datos por un lapso de tiempo de 6 horas.

- Al final de la captura se realiza un filtrado de paquetes por direcciones ip, protocolos.
- Se hace uso del modulo de estadística el cual se genera un listado de equipos conectados a la red en el momento de la captura, además se observa graficas del trafico de red capturado.
- La captura completa se guarda con el formato .pcap

Resultados.

- Uso de la interfaz de la herramienta eficientemente, lo cual se aprecia una interfaz sencilla y fluida para su utilización
- El modulo de estadísticas es completo para ser una herramienta de tipo sniffer, presenta una variedad de funcionalidades, como graficas, listado de equipos por ip y nombres de dominios, estadística por protocolos capturados.
- Archivo .pcap para futuro análisis.

Titulo.

Prueba de sistema de captura de datos Wireshark

Fecha.

Jueves 15 agosto.

Nombre de la herramienta.

Wireshark

Versión.

2.6

Descripción de la herramienta.

Software open source que permite interceptar el trafico en tiempo real, se permite la identificación de paquetes por direcciones ip de los equipos usados en la red, por lo general captura paquetes tcp, udp y icmp, dentro de sus utilidades más importantes es el filtrado de paquetes y en ultimas versiones permite general un pequeña estadística de los paquetes capturados.

Especificaciones técnicas de los equipos utilizados.

Procesador Intel Core i7-8550U CPU 1.80GHz 1.99GHz
RAM 16,0 GB
Tipo de sistema 64 bits

Descripción de la prueba.

- La instalación del software se realizó en horario fuera de oficina, sin embargo la ejecución y captura de paquetes se realiza dentro del horario de oficina, se considera horarios donde el uso de la red es mayor por ejemplo martes de 9am a 4pm.
- Se selecciona la interfaz de red por la cual se hará la captura.
- Se realiza un captura del trafico por más de 6 horas en horario de oficina.
- Durante la captura se intenta inyectar trafico al puerto 80 de un servidor virtual por medio de un ataque sencillo de negación de servicio.

Resultados.

- Uso de la interfaz de la herramienta eficientemente, lo cual se aprecia una interfaz sencilla y fluida para su utilización
- Captura de datos completa acorde al horario estipulado.
- Se logra preciar el comportamiento de la red con la herramienta Wireshark, donde se nota un un trafico fuerte para la el servidor destino que se aplico la prueba.
- Se hace filtrado de información por protocolos y puertos.
- Se aplica estadística a la información capturada primero por equipos de red y después apreciar el consumo de cada uno de los equipos.
- Se realiza un visión de tiempos de respuesta de la maquina que se ataco y se logra apreciar como obtiene muchas solicitudes pero no logra responder a todas, lo cual simula muy bien un ataque de negación de servicio
- Archivo .pcap para futuro análisis.

Titulo.

Prueba de sistema de Nmap entorno gráfico Zenmap

Fecha.

Martes 20 agosto.

Nombre de la herramienta.

Nmap

Versión.

7.70

Descripción de la herramienta.

Nmap es una herramientas de software libre y código abierto que permite la exploración de redes en busca de vulnerabilidades, por medio de la exploración de direcciones ip, servicios y puertos en los objetivos predefinidos.

Especificaciones técnicas de los equipos utilizados.

Procesador Intel Core i7-8550U CPU 1.80GHz 1.99GHz
RAM 16,0 GB
Tipo de sistema 64 bits

Descripción de la prueba.

- Se instala la herramienta Nmap con el entorno grafico Zenmap, la instalación se hace en Linux.
- La instalación del software se realizó en horario fuera de oficina, sin embargo la ejecución y exploración de objetivos se realiza dentro del horario de oficina, se considera horarios donde el uso de la red es mayor por ejemplo martes de 9am a 4pm.
- En la primera ejecución se procede a conocer los diferentes paneles los cuales tiene la interfaz principal.
- Se procede a ejecutar la primera exploración a un objetivo de la red, el cual es una computadora ubicada en la oficina de informática para pruebas.

Titulo.

Prueba de sistema de Nmap entorno gráfico Zenmap

Fecha.

Miercoles 21 de agosto.

Nombre de la herramienta.

Nmap

Versión.

7.70

Descripción de la herramienta.

Nmap es una herramientas de software libre y código abierto que permite la exploración de redes en busca de vulnerabilidades, por medio de la exploración de direcciones ip, servicios y puertos en los objetivos predefinidos.

Especificaciones técnicas de los equipos utilizados.

Procesador Intel Core i7-8550U CPU 1.80GHz 1.99GHz
RAM 16,0 GB
Tipo de sistema 64 bits

Descripción de la prueba.

- Para la prueba de Nmap dentro del horario de trabajo se procede con la exploración de un servidor, el cual ofrece un sistema de almacenamiento en red, con el objetivo de observar cuales puertos tiene habilitados y datos generales del sistema operativo a usar.
- La ejecución se realiza por un tiempo determinado de media hora, importante aclarar que el tiempo de una prueba de este tipo puede depender de las especificaciones técnicas que cuenta el equipo que ejecuta Nmap y de anchos de banda de la red local.

Titulo.

Prueba de sistema de Wireshark y Nmap

Fecha.

Jueves 29 agosto

Nombre de la herramienta.

Wireshark y Nmap

Descripción de la herramienta.

Wireshark: Software open source que permite interceptar el trafico en tiempo real, se permite la identificación de paquetes por direcciones ip de los equipos usados en la red, por lo general captura paquetes tcp, udp y icmp, dentro de sus utilidades más importantes es el filtrado de paquetes y en ultimas versiones permite general un pequeña estadística de los paquetes capturados.

Nmap: Es una herramientas de software libre y código abierto que permite la exploración de redes en busca de vulnerabilidades, por medio de la exploración de direcciones ip, servicios y puertos en los objetivos predefinidos.

Especificaciones técnicas de los equipos utilizados.

Procesador Intel Core i7-8550U CPU 1.80GHz 1.99GHz
RAM 16,0 GB
Tipo de sistema 64 bits

Descripción de la prueba.

- Se realiza la ejecución de Wireshark para analizar la red por medio de la captura de datos.
- Se logra observar un uso amplio de la red donde la captura de paquetes en tan solo 10 minutos de ejecución el trafico de red es constante y un gran numero de equipos ejecutándose.
- Se aprecia un equipo de la red local ejecutando gran cantidad de solicitudes de conexión a otro equipo de la red local, lo cual se procede con verificar la dirección ip.
- Seguido se usa la aplicación Nmap para realizar la exploración de la dirección ip a ubicar.
- Se logra identificar y muestra que es una cámara ip que realiza solicitudes de conexión con un servidor de grabación de video vigilancia usado con anterioridad para pruebas
- El uso de Wireshark e implementación en conjunto con Nmap es útil y potente.

Titulo.

Prueba de sistema de EtherApe

Fecha.

Lunes 9 Septiembre

Nombre de la herramienta.

EtherApe

Versión.

0.9.18

Descripción de la herramienta.

Es una herramienta de monitoreo de la red de forma grafica, permite la visualización de protocolos por color, muestra la actividad de la red en 3 modos distintos en modo Ip, nombre del host y trafico tcp, además proporciona la lectura de trafico de red en tiempo real y por medio de una archivo.

Especificaciones técnicas de los equipos utilizados.

Procesador Intel Core i7-8550U CPU 1.80GHz 1.99GHz
RAM 16,0 GB
Tipo de sistema 64 bits

Descripción de la prueba.

- La instalación y puesta en marcha de la herramienta en Linux es muy secillo se realiza a base de comandos, una vez instalado se procede a la ejecución.
- En el proceso de ejecución la aplicación muestra el trafico de red desde el equipo donde se ejecuta hacia los demás equipos que interactúan en la red.
- La captura es muy grafica y se logra visualizar la interacción de la red por medio de un mapa donde se muestra por color cada uno de los protocolos presentes y el consumo de Bits por segundo de cada uno.
- La prueba se realiza en horario de oficina para una mayor apreciación del uso de la red de datos local.

Titulo.

Prueba de sistema de Wireshark, Nmap y EtherApe

Fecha.
Martes 17 septiembre

Nombre de la herramienta.

Wireshark, Nmap y EtherApe

Descripción de la herramienta.

Wireshark: Software open source que permite interceptar el trafico en tiempo real, se permite la identificación de paquetes por direcciones ip de los equipos usados en la red, por lo general captura paquetes tcp, udp y icmp, dentro de sus utilidades más importantes es el filtrado de paquetes y en ultimas versiones permite general un pequeña estadística de los paquetes capturados.

Nmap: Es una herramientas de software libre y código abierto que permite la exploración de redes en busca de vulnerabilidades, por medio de la exploración de direcciones ip, servicios y puertos en los objetivos predefinidos.

EtherApe: Es una herramienta de monitoreo de la red de forma grafica, permite la visualización de protocolos por color, muestra la actividad de la red en 3 modos distintos en modo Ip, nombre del host y trafico tcp, además proporciona la lectura de trafico de red en tiempo real y por medio de una archivo.

Especificaciones técnicas de los equipos utilizados.

Procesador Intel Core i7-8550U CPU 1.80GHz 1.99GHz
RAM 16,0 GB
Tipo de sistema 64 bits

Descripción de la prueba.

- Con la ejecución de las tres herramientas tiene por objetivo realizar una captura de datos en tiempo real tanto en Wireshark como con EtherApe, en el caso de Nmap para explorar un objetivo especifico de las capturas realizadas.
- Al empezar la captura con Wireshark también se ejecuta EtherApe con la idea de visualizar gráficamente el monitoreo, se logra visualizar una constante comunicación del equipo anfitrión con distintas fuentes de datos remotos, además de enlaces creados con los servidores locales.
- Se visualiza en una herramienta los paquetes consumidos por equipo y en la otra se visualiza graficamente el trafico generado por cada uno de los equipos.

- Con Nmap se hace un exploración intensiva a los equipos locales con los cuales existe mayor interacción.

Anexo # 2

UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

Evaluación de herramientas TIC para gestionar el monitoreo y análisis de la red de datos, Universidad de Costa Rica, Recinto de Golfito, 2019

Propósito:
El siguiente cuestionario tiene como objetivo realizar un diagnóstico de conocimientos y prácticas acerca del uso de herramientas TIC para el monitoreo y analisis red de datos. Con base en los resultados se pretende evaluar las herramientas recomendadas y aplicarlas en laboratorios virtuales.

La información recopilada será utilizada con fines académicos, para obtener el grado de Maestria. Además, los resultados obtenidos podrán ser publicados en forma de un artículo científico, pero preservando la confidencialidad de las personas involucradas.

Instrucciones:
A continuación se presentan una serie de preguntas en las que se deberá responder de forma libre lo que se le solicita. Las respuestas son manejadas de forma confidencial.

¿Cuántos años tiene?

( ) 25-29 años
( ) 30-34 años
( ) 35-40 años
( ) 41-45 años
( ) Más de 45 años

Indique su sexo:

( ) Hombre

( ) Mujer

Seleccione el grado académico superior que posee:

( ) Bachillerato

( ) Licenciatura

( ) Maestría

( ) Doctorado

Anote el nombre de la(s) unidades(s) academica(s) que representa:

_____

_____

¿Cuántos años tiene de laborar en la U.C.R.?

( ) De 1 a 3 años

( ) De 4 a 6 años

( ) Más de 6 años. Especifique: _____

Seleccione el concepto de Tecnologías de la Información y la Comunicación (TIC)

A. Plataforma tecnológica que colabora con el usuario para crear y mantener información por medio de computadoras.
B. Aquellas herramientas computacionales e informáticas que procesan, almacenan, sintetizan, recuperan y presentan información representada de la más variada forma.
C. Lenguaje de computación utilizado para realizar programas y ayudas por medio de tecnologías informáticas.
D. Uso de Internet y la computadora para crear, procesar, almacenar, sintetizar, recuperar y mostrar la información.

Considera importante usar algun software para el control y monitoreo de la red de datos y plataforma informática en general a su cargo.

A. Si, cual _____

B. No

Que opinión merece las diferentes herramientas de software libre existentes para el control, monitoreo y analisis de la red de datos.

_____

_____

_____

_____

Actualmente conoce algun software libre o propetiario para el control, monitoreo y analisis de la red de datos?

A) Si, cual _____

B) **No**

¿Utiliza usted herramientas TIC para el monitoreo y analisis de red de datos?

( ) Sí

( ) No

Indique ¿cuáles herramientas utiliza?

_____

_____

_____

_____

_____

¿Cómo aprendió a usar las herramientas?

( ) Autoaprendizaje

( ) Capacitación.

( ) Otra. Especifique _____

¿Cuáles herramientas TIC para monitoreo y analisis, le interesaría aprender a

usar para implementarlo en su trabajo?

_____

_____

_____

¿Consideras importante alguna capacictación sobre herramitas TIC para el monitoreo y analsis de la red de datos?

_____

_____

_____

En una escala del 1 al 5 donde 1 es el menos importante y 5 el más importante, marque con una X la opción que considere de mayor prioridad en las actividades como RID:

	1	2	3	4	5
Soporte y mantenimiento					
Gestión de activos					
Seguridad y privacidad de la información					
Analisis de datos para la toma de decisiones					
Atención de usuarios					

¡Muchas gracias por su colaboración!